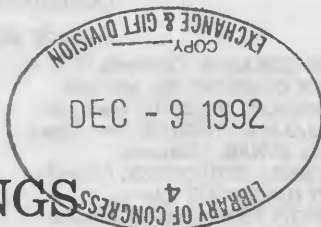


THE THREAT OF FOREIGN ECONOMIC ESPIONAGE TO U.S. CORPORATIONS



HEARINGS BEFORE THE SUBCOMMITTEE ON ECONOMIC AND COMMERCIAL LAW OF THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED SECOND CONGRESS

SECOND SESSION

APRIL 29 AND MAY 7, 1992

Serial No. 65



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

59-313 CC

WASHINGTON : 1992

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

ISBN 0-16-039601-8

COMMITTEE ON THE JUDICIARY

JACK BROOKS, Texas, *Chairman*

DON EDWARDS, California
JOHN CONYERS, JR., Michigan
ROMANO L. MAZZOLI, Kentucky
WILLIAM J. HUGHES, New Jersey
MIKE SYNAR, Oklahoma
PATRICIA SCHROEDER, Colorado
DAN GLICKMAN, Kansas
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
EDWARD F. FEIGHAN, Ohio
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
HARLEY O. STAGGERS, JR., West Virginia
JOHN BRYANT, Texas
MEL LEVINE, California
GEORGE E. SANGMEISTER, Illinois
CRAIG A. WASHINGTON, Texas
PETER HOAGLAND, Nebraska
MICHAEL J. KOPETSKI, Oregon
JACK REED, Rhode Island

HAMILTON FISH, JR., New York
CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois
F. JAMES SENSENBRENNER, JR., Wisconsin
BILL MCCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
CRAIG T. JAMES, Florida
TOM CAMPBELL, California
STEVEN SCHIFF, New Mexico
JIM RAMSTAD, Minnesota
GEORGE ALLEN, Virginia

JONATHAN R. YAROWSKY, *General Counsel*

ROBERT H. BRINK, *Deputy General Counsel*

JAMES E. LEWIN, *Chief Investigator*

ALAN F. COFFEY, JR., *Minority Chief Counsel*

SUBCOMMITTEE ON ECONOMIC AND COMMERCIAL LAW

JACK BROOKS, Texas, *Chairman*

DON EDWARDS, California
JOHN CONYERS, JR., Michigan
ROMANO L. MAZZOLI, Kentucky
MIKE SYNAR, Oklahoma
DAN GLICKMAN, Kansas
EDWARD F. FEIGHAN, Ohio
HOWARD L. BERMAN, California
HARLEY O. STAGGERS, JR., West Virginia
JOHN BRYANT, Texas

HAMILTON FISH, JR., New York
HENRY J. HYDE, Illinois
LAMAR S. SMITH, Texas
CRAIG T. JAMES, Florida
TOM CAMPBELL, California
CARLOS J. MOORHEAD, California

CYNTHIA W. MEADOW, *Counsel*

CHARLES E. KERN II, *Minority Counsel*

KF 27
J862
1992C
COPY 2

CONTENTS

HEARINGS DATES

April 29, 1992	Page 1
May 7, 1992	159

OPENING STATEMENT

Brooks, Hon. Jack, a Representative in Congress from the State of Texas, and chairman, Subcommittee on Economic and Commercial Law	1
--	---

WITNESSES

Fischer, Addison M., president, Fischer International Systems Corp.	280
Gates, Robert M., Director, Central Intelligence Agency	53
Hearn, Dr. James J., Deputy Director, Information Systems Security, National Security Agency	77
Ingram, Kenneth G., director, product development, American Telephone & Telegraph Co.	271
Levchenko, Stanislav	142
Lyons, Dr. John W., Director, National Institute of Standards and Technology, accompanied by James Burrows, Director, Computer Systems Laboratory	163
Myhrvold, Dr. Nathan P., vice president, Advanced Technology and Business Development, Microsoft Corp.	244
Phelps, Marshall C., Jr., vice president, commercial and industry relations, IBM Corp.	130
Riesbeck, James E., executive vice president, Corning, Inc.	121
Rivest, Dr. Ronald L., professor of computer science, Massachusetts Institute of Technology	204
Sessions, William S., Director, Federal Bureau of Investigation	34
Socular, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office, accompanied by Robyn Stewart-Murray, investigator, Office of Special Investigations; Harold Podell, Assistant Director, Information Management and Technology Division; and Gerard S. Burke, expert consultant	6
Turner, Geoffrey W., senior consultant, information security program, Stanford Research Institute International	187
Walker, Stephen T., president, Trusted Information Systems, Inc.	219

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARINGS

American Bankers Association: Prepared statement	229
Brooks, Hon. Jack, a Representative in Congress from the State of Texas, and chairman, Subcommittee on Economic and Commercial Law:	
Excerpt from the CIA report entitled "Japan 2000"	93
Letter dated April 28, 1992, from Hon. Frank Horton, a Representative in Congress from the State of New York, and ranking minority member, House Committee on Government Operations	96
Letter dated June 12, 1991, from Chairman Brooks to Hon. William H. Webster, Director, Central Intelligence Agency, and the July 16, 1991, response	101
Fischer, Addison M., president, Fischer International Systems Corp.:	
Prepared statement	284
Response to Mr. Brooks' questions for the record	328

IV

	Page
Gates, Robert M., Director, Central Intelligence Agency:	
Prepared statement	55
Response to Mr. Brooks' question for the record	120
Summary of CIA report entitled "Japan 2000"	90
Glickman, Hon. Dan, a Representative in Congress from the State of Kansas:	
Letter dated April 10, 1992, from multiple signatories to Chairman Jack Brooks, regarding the Federal Bureau of Investigation's digital telephony proposal	110
Hearn, Dr. James J., Deputy Director, Information Systems Security, National Security Agency:	
Prepared statement	79
Response to Mr. Brooks' question for the record	121
Ingram, Kenneth G., director, product development, American Telephone & Telegraph Co.:	
Prepared statement	273
Response to Mr. Brooks' questions for the record	324
Revised response to a question by Mr. Brooks	318
Levchenko, Stanislav: Prepared statement	144
Lyons, Dr. John W., Director, National Institute of Standards and Technology, accompanied by James Burrows, Director, Computer Systems Laboratory:	
Prepared statement	166
Response to Mr. Brooks' questions for the record	177
Myhrvold, Dr. Nathan P., vice president, Advanced Technology and Business Development, Microsoft Corp.:	
Prepared statement	246
Response to Mr. Brooks' questions for the record	320
Phelps, Marshall C., Jr., vice president, commercial and industry relations, IBM Corp.:	
Prepared statement	132
Revised response to a question by Mr. Glickman	153
Riesbeck, James E., executive vice president, Corning, Inc.: Prepared statement	124
Rivest, Dr. Ronald L., professor of computer science, Massachusetts Institute of Technology:	
Prepared statement	207
Response to Mr. Brooks' questions for the record	240
Sessions, William S., Director, Federal Bureau of Investigation:	
Prepared statement	39
Response to Mr. Brooks' question for the record	119
Smith, Hon. Lamar, a Representative in Congress from the State of Texas:	
Prepared statement	162
Socular, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office:	
Prepared statement	9
Response to Mr. Brooks' questions for the record	22
Turner, Geoffrey W., senior consultant, information security program, Stanford Research Institute International:	
Prepared statement	192
Response to Mr. Brooks' questions for the record	236
Walker, Stephen T., president, Trusted Information Systems, Inc.:	
Prepared statement	222
Response to Mr. Brooks' questions for the record	242

APPENDIXES

Appendix 1.—Draft legislative proposals by the Federal Bureau of Investigation on which several witnesses were asked to comment	333
Appendix 2.—Letter dated May 6, 1992, from multiple signatories to Chairman Jack Brooks, regarding the Federal Bureau of Investigation's digital telephony proposal	350
Appendix 3.—Letter dated September 18, 1992, from John D. Posesta, David R. Johnson, and Jerry Berman, Electronic Frontier Foundation, Inc., regarding the Federal Bureau of Investigation's digital telephony proposal	353

Appendix 4.—Sample letter dated July 28, 1992, from Chairman Brooks to several witnesses requesting comments on FBI Director Sessions' June 4, 1992, letter regarding General Accounting Office testimony on the FBI proposed digital telephony legislation	364
Appendix 5.—Responses to letter in appendix 4:	
Fischer, Addison, president, Fischer International Systems Corp., letter dated September 21, 1992	369
Ingram, K.G., director, product development, American Telephone & Telegraph Co., letter dated September 15, 1992	373
Myhrvold, Dr. Nathan P., vice president, advanced technology and business development, Microsoft Corp., letter dated August 17, 1992	376
Rivest, Dr. Ronald L., professor of computer science, Massachusetts Institute of Technology, letter dated November 1, 1992	381
Turner, Geoffrey W. Turner, SRI International, letter dated August 20, 1992	383

CERTAIN STAFFING AND CERTAIN BUDGET

My friend, The committee will have to order today for today our hearings to consider the threat of foreign espionage, particularly in U.S. corporations by both their domestic and international counterparts.

With the rest of the House, Congress, the staff will have given us a new set of global corporate espionage and security. As a result, we need to conduct our country's economic security in order to protect U.S. corporations in the international market.

Now, clearly the role of scientific research, information and technology is crucial in foreign government, with its economic weapons, including their own security and political systems in world markets. Intelligence operations are being being the nations and the world in Europe and the Far East, as well as targeting U.S. corporations. The information they seek is not simply technological data but also financial and commercial information which will give access to our nation's future in the world market.

The staff has found that U.S. companies have lost billions of dollars through the theft of commercial secrets and technical property. They believe that the threat of foreign espionage is a serious problem, particularly in the area of scientific, technological and financial information and that the U.S. must take action to protect its economic security.

THE THREAT OF FOREIGN ECONOMIC ESPIONAGE TO U.S. CORPORATIONS

WEDNESDAY, APRIL 29, 1992

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ECONOMIC AND COMMERCIAL LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2141, Rayburn House Office Building, Hon. Jack Brooks (chairman of the subcommittee) presiding.

Present: Representatives Jack Brooks, Don Edwards, John Conyers, Jr., Romano L. Mazzoli, Dan Glickman, Hamilton Fish, Jr., Carlos J. Moorhead, Henry J. Hyde, Lamar S. Smith, and Craig T. James.

Full committee staff present: James E. Lewin, chief investigator; John D. Cohen, investigator; Daniel M. Freeman, counsel; Teresa Faunce, research assistant; Charles E. Kern II, minority counsel; and Cordia Strom, minority counsel.

OPENING STATEMENT OF CHAIRMAN BROOKS

Mr. BROOKS. The subcommittee will come to order. Today we begin our hearings to consider the threat of foreign economic espionage to U.S. corporations in both their domestic and international operations.

With the fall of the Soviet Government, the cold war has given way to a new era of global competition in trade and finance. As a result, we need to protect our country's economic resources in order to maintain U.S. competitiveness in the international economy.

Now, clearly the risks to sensitive business information are dramatically increasing as foreign governments shift their enormous espionage resources away from military and political targets to world commerce. Intelligence agencies from the former Soviet bloc nations and our allies in Europe and the Far East are actively targeting U.S. corporations. The information they seek is not simply technological data but also financial and commercial information which will give overseas competitors a leg up in the world marketplace.

The GAO has found that U.S. companies have lost billions of dollars through the theft of commercial secrets and intellectual property. They believe, as I do, that unless the United States deals aggressively with this problem, it will undermine our country's ability to compete internationally and threaten our Nation's long-term economic survival.

Fortunately, advances in encryption technology offer U.S. industry new protections against unauthorized access to sensitive business information. Using a system of encryption codes and electronic keys, American companies can now send new product, engineering, and design information across international telecommunications networks without fear that foreign intelligence services may eavesdrop and provide that information to foreign competitors.

However, as is often the case, this technological breakthrough carries some problems with it as well. U.S. intelligence and law enforcement agencies are fearful that if encryption technology becomes readily available, it would be used by terrorists, drug dealers, and others to shield their activities from Government scrutiny and prosecution. Apparently, some of these agencies believe that the Federal Government must restrict the use of this technology to ensure that they will be able to listen in or intercept electronic communications involving these types of activities.

Now leaders of U.S. industry, on the other hand, believe that the intelligence and law enforcement agencies are unfortunately misguided in their attempts to stop the inevitable progress of encryption technology, especially since it is, they say, already available worldwide. They argue that the use of this technology is crucial to U.S. corporations if they are going to be able to protect their trade secrets and remain competitive in the world marketplace.

While there is no question that the concerns raised by the intelligence community over the advances in encryption technology need to be addressed, I firmly believe that we must encourage an open and robust debate on this issue by broader segments of our society before any final decisions are made. I also believe that Congress needs to review carefully any proposals to expand the authorities of the CIA and the NSA in order to combat the foreign economic espionage threat.

I would be particularly concerned about a suggestion that these agencies should be given responsibilities already and currently assigned by statute to the FBI and other executive branch agencies. So I look forward to discussing these issues with our witnesses today, and we will have—I'll just tell you now—panel one with Milton Socolar, who will lay out briefly the case that we have from the GAO, and on panel two we will have our very distinguished Director of the FBI, Judge Sessions, Director of the CIA, Robert Gates, and James Hearn for the Department of Defense. On panel three we will have corporate representatives: James Riesbeck from Corning, Marshall Phelps from IBM, and Stanislav Levchenko, formerly a KGB agent. That is the way we will set it up.

With that, I would like to yield to the distinguished minority member, Mr. Fish from New York.

Mr. FISH. Thank you, Mr. Chairman, and I'll be very brief since you have covered the areas that we will be dealing with.

I'm delighted to welcome our distinguished witnesses today. Foreign economic espionage against U.S. companies both here and abroad is an ever increasing problem which, as you said, directly impacts U.S. economic and security interests. So it is vital that we understand the nature and the extent of the problem so we can develop solid policy to protect U.S. companies.

As even our traditional allies are involved in economic espionage, we must carefully balance foreign policies, economic, and security interests to determine to what degree there will be U.S. Government involvement and under what circumstances. I commend you for scheduling this hearing and look forward to the testimony.

Mr. BROOKS. Mr. Edwards, the gentleman from California.

Mr. EDWARDS. Mr. Chairman, as you know, I have an urgent other commitment, and I have to leave. I sincerely regret that I can't stay very long, because this is a very important subject. I compliment the chairman on his statement, my views correspond with his. I also compliment Director Sessions who, in his statement, which I have read, shows some hesitation and care in addressing this very important subject, because I have a great concern about this subject. Coming from Silicon Valley, I recognize the fact that we have had nothing but trouble the last few years with export licenses, where the Pentagon and some intelligence agencies are involved in whether or not these export licenses are issued. Our manufacturers are trying to sell innocent goods much of the time overseas, but when their export licenses are held up, the Japanese or the Germans or the Swiss make the sales.

Now I'm not just talking through my hat, Mr. Chairman. The National Academy of Sciences in 1987 said that these export license holdups, where you get the Government involved in dealing with sales of manufacturers overseas of American products, cost \$9.3 billion per year. That is the money that the National Academy of Sciences says our manufacturers are losing yearly because Government involves itself in these sales unnecessarily.

So, with that, I'm pleased with your statement and, of course, with Mr. Fish's. Thank you.

Mr. BROOKS. Thank you.

Mr. Smith, the gentleman from Texas.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, I, too, appreciate the attention this committee is giving to this very important subject, and it is very clear to me that our goal today is to not only point to the problems that are inherent in the economic espionage but also to the solutions as well. We can't overlook the problems; when over a third of U.S. firms say they have been the target of economic espionage, the problem is clear.

Mr. Chairman, I also want to make a point this morning of giving a special welcome to a personal friend from San Antonio, Director Bill Sessions, who is the Director of the FBI, and say that because he is a personal friend I can state to my colleagues on the committee that one of the real reasons that Bill Sessions became Director of the FBI was because of his absolute unquestioned reputation for integrity in San Antonio. He has always been viewed as a pillar of integrity to his friends and even to those who might not agree with him. So it is a special opportunity for the members of this committee, I think, to welcome somebody with that kind of reputation.

Thank you, Mr. Chairman.

Mr. BROOKS. Mr. Conyers, the gentleman from Michigan.

Mr. CONYERS. Thank you, Mr. Chairman.

My congratulations to you for holding this hearing addressing the questions of the post-cold war era: How can we reshape governmental institutions to meet the economic challenges.

The first step might be to reduce this obsession with secrecy that has dominated American Government for so long. I'm amazed that the intelligence agencies are still talking in terms of threats from traditional adversaries when the reality is that our allies, like Japan and Western European countries, are now our new and chief competitors.

So I'm hoping to see an attitude modification on the part of our intelligence agencies that comports with the fact that we are in 1992 and not some pre-World War II circumstance, and I thank you very much for allowing this intervention.

Mr. BROOKS. Thank you, Mr. Conyers.

Mr. Hyde, the gentleman from Illinois.

Mr. HYDE. Thank you, Mr. Chairman.

I did not intend to make an opening statement, but I have listened to my good friend, Mr. Edwards, and my equally good friend, Mr. Conyers, inveigh against governmental intervention to the detriment of our economic life, and I simply would like to add that, in my humble opinion, we need a balance between the needs of commerce, which are indeed important but not necessarily paramount, and the needs of national security, and while indeed it is 1992, there are still some areas in the world that do not wish us well nor feel that we are the answer to everyone's problem.

Export licenses ought to concern the Government, because we are the greatest innovative country in the world in terms of inventions and creating things, but many of these items have military and intelligence aspects to them, implications to them, and I think providing for the common defense is still the first duty of Government, and while Government can be too interventionist and too obstructionist, on the other hand no Government concern about the security implications of what is being exported bothers me even more.

What we need is an enlightened balance between the normal needs of commercial activity and protecting our national security. I am confident that the intelligence agencies and the Department of Defense, subject to the ever present bureaucratic lethargy—I am confident that their intentions, their goals, are to protect the people of this country, and those are very legitimate goals, and I think we ought to bear that in mind as we conduct these hearings.

Thank you, Mr. Chairman.

Mr. BROOKS. Gentlemen, this morning some of our witnesses will appear in panels. For the sake of brevity and since all statements will be made a part of the hearing record in full—pardon me; Mr. James would like to speak.

Mr. James, the gentleman from Florida.

Mr. JAMES. Thank you so much, Mr. Chairman.

Mr. BROOKS. Mr. Moorhead, did you want to speak also?

Mr. MOORHEAD. Yes, Mr. Chairman.

Mr. BROOKS. All right. And, Mr. Glickman, we will get to you, too—everybody.

Mr. JAMES. I'm quite frankly concerned about expanding jurisdiction of the CIA or any agency with the mission and with the cloak of secrecy that many times is applicable and appropriate when it

comes to military considerations in defense of this country. But to invade and go into economic considerations, whether you label it economic espionage or otherwise, we are crossing over a line that I'm not sure we want to cross without a specific and very clear clarification as to what are the duties and what are the disclosures that would be involved in that type of activity.

I can't see the same statutes that would protect the CIA from disclosing certain facts and relevant information being applicable in this division of their activity. I see they are light years away from what your previous perceived responsibilities and duties are.

Likewise, this would be a very direct but hidden cost to business, to the taxpayer, under the guise of economic espionage or protecting business interests when we consider the international aspect of business and foreign ownership of stock, foreign control, and sometimes you can't even determine either of those. Just look at the components of a car, and you will see already how involved internationally many products are.

So I'm afraid of general jurisdiction being expanded in such a way unless we are very careful to specify exactly what we are talking about in regard to economic espionage and obviate or exclude from the protections that the CIA otherwise might have in regard to the defense of this country. So I will be listening carefully to the testimony, and I wish I could be here all morning and listen to it; so I will have to read it after you have given it in many cases.

Thank you so much.

Mr. BROOKS. Mr. Glickman, the gentleman from Kansas.

Mr. GLICKMAN. Thank you, Mr. Chairman.

Along with Mr. Hyde, I have had the privilege of serving and continue to serve on the Intelligence Committee where Judge Sessions and Director Gates have testified over the growing economic threat to America, and economic intelligence is clearly becoming a new priority of the intelligence community as we move into a post-cold war era.

There are a couple of issues I would hope the panels could address. One is foreign governments' targeting American companies, stealing American private secrets, for national security or economic purposes.

Then the second part of that equation is foreign companies not necessarily affiliated with foreign governments but perhaps part of a much closer organizational structure than we have in this country doing the same thing.

Also, I would like the witnesses to address whether current statutes are adequate to deal with both of those problems. These may not be intelligence statutes, these may be 18 U.S.C. Criminal Code statutes and civil statutes in terms of piracy and theft.

America is much more at risk today by our industrial base being withered away than it is probably by the former Russian empire, and it is important that this country become lean and mean in fighting the economic threats of the rest of the world, particularly when our companies may be the targets of competitors who would think nothing of stealing secrets in a surreptitious way.

I have skimmed the testimony of Director Sessions and Mr. Gates. They both refer to this in a general fashion, and I know that the Justice Department is looking into this very actively. But this

is a very, very important hearing, and I would hope again that the witnesses could deal with the issue of whether current criminal statutes are effective to deal with a potential problem area.

I yield back my time, Mr. Chairman.

Mr. BROOKS. Mr. Moorhead, the gentleman from California.

Mr. MOORHEAD. Thank you, Mr. Chairman. I want to congratulate you on bringing this subject before the committee today.

I think the question about what role the U.S. Government should play in determining whether we are losing business or losing our trade capability because of espionage by foreign governments or corporations in foreign countries is a very important issue for us to consider.

The survey by the American Society for Industrial Security last year reported that 37 percent of the 165 U.S. firms responding said they had been the target of spying. Coming out of a recession, I think the American people are very cognizant of the importance of jobs to our country, as they are to other countries in the world, and it is important that we protect our own capabilities by the use of the facilities that we have, or else we will find ourselves in more difficulty than we have been economically.

I think it is important for us to learn just exactly what the situation is and to be able to make a determination of what role the Government should play or the FBI should play based on what the actual facts turn out to be.

Thank you, Mr. Chairman.

Mr. BROOKS. Thank you very much.

This morning, for the sake of brevity, all statements are going to be put in the record, and we will ask each witness to give a 5-minute summary of their statement.

Our first witness is Milton J. Socolar, Special Assistant to the Comptroller General. He has served in the General Accounting Office for more years than either he or I would care to admit. I have always valued his friendship, his expertise, and his judgment.

He is accompanied by Ms. Robyn Stewart-Murray, an investigator from the Office of Special Investigations; Howard Podell, Assistant Director of the Information Management and Technology Division; and Gerard S. Burke, an expert consultant who has spent many years in the intelligence community and currently advises corporations on security and counterintelligence matters.

It is good to see you, and welcome to the committee.

STATEMENT OF MILTON J. SOCOLAR, SPECIAL ASSISTANT TO THE COMPTROLLER GENERAL, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY ROBYN STEWART-MURRAY, INVESTIGATOR, OFFICE OF SPECIAL INVESTIGATIONS; HAROLD PODELL, ASSISTANT DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION; AND GERARD S. BURKE, EXPERT CONSULTANT

Mr. SOCOLAR. Thank you very much, Mr. Chairman.

We are pleased to be here today at your request to talk about our ongoing examination of issues involving foreign economic espionage.

From the information that we have gathered in our work, it is very clear to me that these are very important hearings. The prob-

lems that have been referred to this morning are longstanding problems, but they are becoming more pronounced in the light of our economic competition on a global basis.

In a recent speech, Central Intelligence Agency Director Robert Gates focused on the changing activities of foreign intelligence efforts when he reported, "Some foreign intelligence services have turned from politics to economics, and the United States is their prime target." President Bush also expressed concern about such activities when he stated in a speech, "We must thwart anyone who tries to steal our technology or otherwise refuses to play by fair economic rules."

It is not possible for me to quantify the scope of economic espionage conducted by foreign intelligence agencies, but there is evidence of a real and growing problem. It has been known for many years that the KGB has been misappropriating U.S. corporate secrets. Indeed, the FBI has estimated that the efforts of the KGB and its surrogates saved the Soviet Union billions of dollars and years of research and development efforts in gaining Western technologies and expertise.

A former Director of the French Secret Service publicly admitted that he directed French industrial and technological intelligence forces to gather economic information from the United States and other countries. In one instance he stated that the Service compiled a detailed secret dossier of the proprietary proposals from United States and Soviet companies who were competing with a French company for a billion dollar contract to supply fighter jets for India. Negotiators for the French company, which builds the Mirage jet, were stated to have then used the information provided by the Service to obtain the contract.

We have some other examples of economic espionage found in open source documents that further illustrate the nature of the problem. Recon Optical, Inc., a U.S. company, contracted with the Israeli Government to design a top secret airborne spy camera system. After months of disagreement between Recon and Israel, Israeli agents allegedly gave Recon's plans for the system to Electro-Optics, an Israeli defense contractor. Recon brought suit against Israel, and the case was settled in 1991. Arbitration records of the settlement are sealed as part of the settlement agreement.

In two other instances, the French Secret Service was allegedly involved in the misappropriation of proprietary information from two U.S. companies. In the first case, the Service acquired proprietary information for IBM's next generation personal computer. The Service reportedly provided the information to Compagnie des Machines Bull, an IBM competitor in France.

In the second case, a French national working for Corning, Inc., in France sold information and trade secrets to the French Secret Service regarding Corning's latest fiber optic technology. The Service, in turn, allegedly provided this information to a French competitor of Corning.

There is a complicating factor in examining the problem of economic espionage, and that is the difficulty in determining whether a particular theft of information is the result of foreign government or foreign business activity. This occurs when the company perpetrating the theft is in a country where the government-to-indus-

try relationship is substantially different than what prevails in the United States. The government-to-industry relationship in Japan, for example, makes it difficult to determine if the Japanese Government is involved when Japanese companies successfully acquire U.S. corporate secrets in an unauthorized manner.

For example, in 1982 Hitachi employees pleaded guilty in conspiring to transport stolen IBM property—in this case, design documents and components for every major part of IBM's newest and most powerful generation of computers which were not yet on the market. Hitachi, a manufacturer of IBM-compatible products, planned to use this technology to eliminate costly and time-consuming research, thereby shortening the leadtime required to bring compatible Hitachi products to the marketplace.

The clandestine operations by the French and other foreign intelligence agencies can be contrasted sharply with the U.S. intelligence community's view that it should not conduct industrial or economic espionage to benefit U.S. companies. As CIA Director Gates recently stated, U.S. intelligence does not, should not, and will not engage in industrial espionage.

Mr. Gates' position is consistent with the views of U.S. industry leaders. They have stated that it would be highly undesirable to have the CIA engage in this type of activity due to ethical and practical reasons. For example, what would the intelligence community's dissemination policies be with respect to foreign company secrets?

There is a related issue that concerns the security of electronic data transmissions by U.S. companies. Cryptographic and other information technologies exist that can protect against the vulnerability of the electronic transmission of sensitive information. Such technology is readily available under internationally accepted industry standards. U.S. industry could use this technology to afford a high degree of protection to its propriety information.

The intelligence community, however, appears to be insisting upon the development of a different standard for U.S. industry for electronic communications between it and the Government. This separate standard is weaker than what is commercially available, is an added burden on commercial activities, and raises question as to whether any practical purpose would be served by the requirement. The issues involved, although they may lie within the national security area, merit public attention.

The issues that this sort of information brings to the fore, it seems to me, are twofold. One is the extent to which our intelligence agencies should be assisting U.S. business and the extent to which U.S. business should be denied the benefits of the most efficacious technology that is available to protect their proprietary information.

It seems to me that the issues are similar to the issues that were dealt with in enacting the Computer Security Act of 1987 where there was great concern about the Department of Defense insinuating itself into the nonclassified, although sensitive, information control arena.

The current posture seems to be that our intelligence apparatus will not engage in spying to obtain foreign company proprietary data for the benefit of American business but that American busi-

ness is not being allowed to freely use the most advanced transmission technologies that are available to protect their proprietary data. It seems to me that these are issues of grave importance, that they do merit free and open public debate in terms of reaching a national consensus as to how these issues should be dealt with.

I and my colleagues would be glad to answer any questions that you, Mr. Chairman, or other members of the committee may have.

Mr. BROOKS. Thank you very much.

[The prepared statement of Mr. Socolar follows:]

**PREPARED STATEMENT OF MILTON J. SOCOLAR, SPECIAL ASSISTANT
TO THE COMPTROLLER GENERAL, U.S. GENERAL ACCOUNTING OFFICE**

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today at your request to talk about our ongoing examination of issues involving foreign economic espionage.

The theft of U.S. proprietary information or technology by foreign companies has long been a part of the competitive business environment. However, as the world political climate changes with the end of the Cold War, the surreptitious gathering of economic and technological information has taken on added significance. The unauthorized acquisition of U.S. proprietary or other information by foreign governments to advance their countries' economic position is growing--referred to as economic espionage. The loss of proprietary information and technology through espionage activity will have broadening detrimental consequences to both U.S. economic viability and our national security interests.

The United States, a leader in creative technological research and development, is a prime target for economic espionage. In recent months, government officials have begun to speak out about this problem. In a recent speech, Central Intelligence Agency (CIA) Director Robert Gates focused on the changing activities of foreign intelligence efforts when he reported, "[S]ome foreign intelligence services have turned from politics to economics and the United States is their prime target." President Bush also expressed concern about such activities when he stated in a speech,

"We must . . . thwart anyone who tries to steal our technology or otherwise refuses to play by fair economic rules."

Sophisticated and often undetectable methods are used in economic espionage. Unfortunately, U.S. companies targeted by foreign intelligence agencies may not know--and may never know--that they have been targeted or compromised. In addition, many companies that know they have been victimized want to avoid the negative publicity associated with the loss of valuable trade secrets and other proprietary information. Industry representatives are thus reticent to publicize incidents of espionage.

While it is not possible for me to quantify the scope of economic espionage conducted by foreign intelligence agencies, there is evidence of a real and growing problem. It has been known for many years that the KGB has been misappropriating U.S. corporate secrets. Indeed, the FBI has estimated that the efforts of the KGB and its surrogates saved the Soviet Union billions of dollars and years of research and development efforts in gaining Western technologies and expertise.

A former director of the French secret service, DGSE (Direction Generale de la Securite Exterieur), publicly admitted that he directed French industrial and technological intelligence forces to gather economic information from the United States and

other countries. In one instance, he stated that the DGSE compiled a detailed secret dossier of the proprietary proposals from U.S. and Soviet companies who were competing with a French company for a billion dollar contract to supply fighter jets for India. Negotiators for the French company, which builds the Mirage jet, were stated to have then used the information provided by DGSE to obtain the contract.

The following instances of economic espionage that we found in open source documents further illustrate the nature of the problem:

- Recon Optical, Inc., a U.S. company, contracted with the Israeli government to design a top-secret airborne spy-camera system. After months of disagreement between Recon and Israel, Israeli agents allegedly gave Recon's plans for the system to Electro-Optics, an Israeli defense contractor. Recon brought suit against Israel, and the case was settled in 1991. Court records of the settlement are still sealed.
- In two other instances, the French DGSE was allegedly involved in the misappropriation of proprietary information from two U.S. companies. In the first case, the DGSE acquired proprietary information for IBM's next-generation personal computer. The DGSE reportedly provided the information to Campagnes des Machines Bull,

an IBM competitor. In the second case, a French national, working for Corning, Inc. in France, sold information and trade secrets to DGSE regarding Corning's latest fiber optic technology. DGSE, in turn, allegedly provided this information to a French competitor of Corning.

In some instances, U.S. business people have aided foreign competitors in obtaining information. For example, in one case a U.S. scientist sold the trade secrets of U.S. pharmaceutical companies to foreign corporations. The research and development costs associated with the pharmaceutical products alone were estimated at \$750 million.

A complicating factor in examining the problem of economic espionage is the difficulty in determining whether a particular theft of information is the result of foreign government or foreign business activity. This occurs when the company perpetrating the theft is in a country whose government-to-industry relationship is substantially different than what prevails in the United States.

The government-to-industry relationship in Japan makes it difficult to determine if the Japanese government is involved when Japanese companies successfully acquire U.S. corporate secrets in an unauthorized manner. For example, in 1982 Hitachi employees pleaded guilty to conspiring to transport stolen IBM property--in

this case, design documents and components for every major part of IBM's newest and most powerful generation of computers, which were not yet on the market. Hitachi, a manufacturer of IBM-compatible products, planned to use this technology to eliminate costly and time-consuming research, thereby shortening the lead time required to bring compatible Hitachi products to the marketplace.

The clandestine operations by the DGSE and other foreign intelligence agencies can be contrasted sharply with the U.S. intelligence community's view that it should not conduct industrial or economic espionage to benefit U.S. companies. As CIA Director Gates recently stated, U.S. intelligence "does not, should not, and will not engage in industrial [or economic] espionage." Mr. Gates' position is consistent with the views of U.S. industry leaders; they have stated that it would be highly undesirable to have the CIA engage in this type of activity due to ethical and practical reasons. For example, what would the intelligence community's dissemination policies be with respect to foreign company secrets?

Cryptographic and other information technologies exist that can protect against the vulnerability of the electronic transmission of sensitive information. Such technology is readily available under internationally accepted industry standards. U.S. industry could use this technology to afford a high degree of protection to its proprietary information. The intelligence community, however, appears to be insisting upon the development of

a different standard for U.S. industry for electronic communications between it and the government. This separate standard is weaker than what is commercially available, is an added burden on commercial activities, and raises the question as to whether any practical purpose would be served by the requirement. The issues involved, although they may lie within the national security area, merit public discussion.

Technological advances in computers have made it easier for foreign intelligence agencies and others to monitor the electronic commerce of U.S. industry. U.S. companies may be less able to protect themselves from the espionage apparatus of a foreign government than from a competitor. This problem is made more acute by the globalization of economic competition and the use of advanced communication technologies to conduct business. We need to examine openly the extent to which the government should be hampering industry's use of generally available cryptographic technology that would better protect electronic business communications.

The CIA and the Federal Bureau of Investigation (FBI) maintain foreign counterintelligence efforts to protect national security. However, the efforts of these agencies do not appear to be sufficiently coordinated to adequately protect U.S. industry against economic espionage. This suggests that there are significant policy issues requiring resolution. In addition, the

National Security Agency (NSA) maintains electronic intelligence capabilities that may include gathering economic information. Under the Computer Security Act of 1987, NSA's role is to provide technical advice to the National Institute of Standards and Technology (NIST). NIST's responsibility, under the act, includes assisting government agencies and private entities in protecting unclassified, but sensitive, computer data from compromise.

Many of the issues in economic espionage, concerning the roles of the FBI and CIA, are similar to those raised during the hearings leading to the enactment of the Computer Security Act of 1987. A wide range of concerns had been raised at that time, regarding President Reagan's decision to give the Department of Defense (DOD) responsibility for computer security involving unclassified, but sensitive, data located in civilian agencies and the private sector.

As you know, Congress responded by holding hearings that resulted in legislation giving the responsibility to the Commerce Department instead of DOD. Pursuant to the act, the Commerce Department is responsible for issuing computer security standards that allow industry to use the best commercially available technology.

In closing, economic espionage is an important problem that this country has to face. The criminal justice and intelligence

agencies have not adequately addressed this problem. Economic espionage must be looked at very carefully. There should be a thorough review of which agencies should be involved in this area together with what their responsibilities should be. No decision should be made without benefit of a full public debate. Currently, most of the discussions are being conducted within the intelligence community, without the benefit of public debate. In the final analysis, Congress may have to develop legislation to protect industry from economic espionage. How these issues are decided may have a dramatic effect on the economic future of this country.

This concludes my prepared statement. We would be pleased to answer any questions you may have.

Mr. BROOKS. Do you agree that efforts by the U.S. intelligence agencies to restrict the use of cryptographic technology will adversely affect the ability of American corporations to protect their trade secrets and compete internationally?

Mr. SOCOLAR. Yes, I do, Mr. Chairman. The availability of that technology is very, very sound, and if the American business is going to be required to use weaker technology, it would not have the same high degree of assurance that its proprietary data won't be compromised.

Mr. BROOKS. Could you explain the difficulties that GAO had in getting access to information from the FBI and the CIA while conducting your investigation of economic espionage?

Mr. SOCOLAR. Information access was a significant problem for us. Each of the agencies told us that information on economic espionage is considered classified, that access was going to be difficult to provide on this basis. The CIA initially went so far as to say that it was their belief that they weren't really accountable to us, that with regard to congressional oversight, citing the Intelligence Oversight Act of 1980, the CIA said that they were only accountable to the House and the Senate Intelligence Committees.

Eventually, the CIA did provide us a general briefing on the issue but was quite limited on the basis that they indicated they wanted to avoid divulging sources and methods.

The FBI refused to cooperate with GAO fundamentally, I think, because it has been a longstanding position of the FBI that our Office of Special Investigations does not have the authority to conduct this kind of investigation, that criminal investigations are really within the domain of the executive branch.

Mr. BROOKS. You know the courts have consistently held that Congress can investigate any allegation of wrongdoing within the executive branch, regardless of whether it involves administrative, civil, or criminal wrongdoing. The OSI, Office of Special Investigations, was created at GAO at my request some years ago and, I think, it has been effective in trying to determine wrongdoing and mismanagement within some of the executive agencies.

Mr. Burke, you have 25 years experience working with U.S. intelligence agencies and 13 years advising companies. Would you tell the subcommittee which countries, in your judgment, are most notorious for trying to steal U.S. trade secrets and give us an assessment of their activities.

Mr. BURKE. Yes, Mr. Chairman. Thank you.

I'm able to speak to this subject today primarily because of my current activity as a consultant to industry and my experience in industrial counterespionage since leaving Government 14 years ago. My consulting firm has considerable hands-on experience with actual, real-life industrial espionage cases. And my observations are also derived from associations with colleagues in the same industrial counterespionage business in the United States and elsewhere around the world.

But while it is the private sector from whence I come now, I should note that 20 years ago, when I headed the staff of the President's Foreign Intelligence Advisory Board, that Board performed a very comprehensive study of economic intelligence at the personal direction of the President. We recommended a number of changes

in the structure and wiring diagram of the intelligence apparatus, but our most important conclusion or finding at that time, in my judgment, was a conceptual one when the Board said, "From this moment forward, economic intelligence must be considered a vital function of the national security and must be accorded priority at least equal to military and diplomatic intelligence."

We also volunteered another observation to the President. In the area of commercial intelligence, we said that while American companies need information of a tactical nature that would give them an edge when competing in the world marketplace, we did not believe that it was appropriate that the U.S. Government should provide that intelligence; the user companies should acquire it themselves.

In this respect, the United States was and is unique. Among the world's industrialized nations, the United States alone does not use its governmental intelligence apparatus to systematically support individual private companies with competitively valuable intelligence. To do so, the Board believed at that time, would run contrary to our legal, ethical, and cultural traditions. Moreover, from a purely pragmatic viewpoint, it would be extremely difficult to do so and would not be worth the attendant agony. And, as you know, Mr. Chairman, these very same points are now being debated all these 20 years later.

These kinds of inhibitions don't occur in any other industrialized nation. The practice of using intelligence to directly support business has never even been an issue in Communist states, where corporate customers of competitively valuable data are, in fact, part of the government itself. It is merely a question of one branch of the bureaucracy collecting the information and another branch consuming it.

In the former Soviet Union, economic intelligence has long enjoyed the highest priority. The target was not simply Western technological data which would help Soviet industry but was also financial and commercial information which gave the Soviets a variety of advantages in the world marketplace.

It remains to be seen how, not whether, the successor states in the Commonwealth of Independent States will proceed along similar tracks. With their increasingly dire economic situations and the overwhelming need to play a variety of catchup ball, it is hard to imagine that Russia and the other states will not accord the very highest priority to these kinds of intelligence requirements.

Within the last week, French authorities reported breaking up an industrial espionage ring working for Moscow, apparently in both France and Belgium, which may have been after French telecommunications information. France arrested one Belgian and four Frenchmen. Two weeks earlier, Belgium expelled four Russians connected with the same case. This is just this month.

Evidently, this industrial spy ring was founded in the 1970's and has been operating ever since. The disturbing, but not unexpected, thing is that it seems to have continued operations in spite of the breakup of the Soviet Union and the transfer of foreign intelligence activities out of the KGB into a resubordinated organization. And it continued to be active notwithstanding the efforts by Russia to obtain Western help legitimately.

An apparently similar but unrelated case has also just become public in the Netherlands, which announced last week that it, too, had expelled four Russians for industrial espionage.

So while it is too early to make any definitive projection as to how the end of the cold war will affect the intensity of Russian economic espionage, the smart money says it will certainly not diminish. Whether the same is true for former Soviet client states, such as Czechoslovakia and Poland, also remains to be seen.

If anything, Communist China has been even more aggressive. China is not overburdened with scruples about the means it employs to collect economic and commercial information. It uses a continual full court press; anything goes. Few Chinese citizens bound for the West exit their country without explicit orders to acquire in any way possible the data which will help their nation compete in global commerce.

Japan, of course, has received a great deal of press about its commercial intelligence operations. And while it does indeed use classical industrial espionage methodologies, as it demonstrated in the infamous IBM-Hitachi case of the early 1980's, the principal characteristics of the Japanese economic competitive intelligence effort is its massiveness, including a very large scale, comprehensive, overt collection and analysis activity.

As Mr. Socolar has indicated, France is a close second to Japan in terms of the notoriety which its economic intelligence operations have received in the international media. By the admission of senior French officials, commercial intelligence, with emphasis on the technological variety, has enjoyed the highest priority for at least the last decade and probably longer. The French use a wide range of intelligence tradecraft, from second-story black bag jobs to classic, long-term human penetrations, to a very heavy reliance on technical intelligence.

Israelis, too, appear to emphasize the acquisition of high-tech industrial intelligence, and, like the French, they are paid to employ a diversity of collection methodologies that are prone to discovery and exposure. The likelihood of diminishing American financial assistance is apt to increase their perceived dependence on commercial intelligence.

Historically, the Swedes and the Swiss have used commercial intelligence primarily for the collection and analysis of information of a fundamentally financial nature. Their efforts are characterized by a high degree of organization and structure.

The United Kingdom may have the most professional and successful effort of all. British activities appear to the private sector to be systematized, technically sophisticated, subtle, and eminently discreet. The British almost never get caught when operating in the economic commercial zone of intelligence, and they fully exploit the access provided by a long history of colonization alliances. Like the Japanese, they understand the enormous power of intelligence and the extent to which it can even the odds when competing with countries much larger in size and physical resources.

Various other nations, too numerous to mention here, conduct economic and commercial intelligence activities, using private or private sector intelligence organizations.

Mr. CONYERS [presiding]. Mr. Burke, could you wind it up, please, so we can get to the questions.

Mr. BURKE. Yes. I would conclude by saying that although economic and commercial intelligence has been around for centuries and indeed has been long at the core of certain national intelligence systems, we are only now, with the end of the cold war, beginning to perceive the ubiquity of this effort worldwide.

Thank you.

Mr. CONYERS. Thank you very much.

Mr. Socolar, do you believe the FBI, the CIA, and the National Security Agency are the best ones for dealing with the threats to American corporations from foreign espionage?

Mr. SOCOLAR. I think that they would certainly have to be a part of the picture in providing to U.S. industry information that may have a bearing on the loss of proprietary information by various companies. The question gets a little more difficult when it gets to the issue of international agencies overtly and actively seeking the information from foreign companies to provide to U.S. companies, and I think, too, that it is extremely important to provide to U.S. industry the best means available for industry itself to protect its own information.

Mr. CONYERS. Do you think we need a new agency to look at this question outside the traditional intelligence community when it comes to the private sector?

Mr. SOCOLAR. I wouldn't hazard an opinion on that question. I would have to say at this point that I don't really have answers to the issues that this whole situation gives rise to. The important thing is for the issues to be aired, for the kinds of considerations that are involved to be debated, and for some kind of conclusion to be reached through that process rather than to have the intelligence communities operating, say, behind closed doors and resolving these issues without that open debate.

Mr. CONYERS. Do you think the intelligence community is right in opposing industry's efforts to protect their data by using new technologies such as encryption codes?

Mr. SOCOLAR. That seems to me, from what I know about the situation, to be a losing battle, that ultimately with this kind of technology available literally worldwide, it seems to me that it is going to be difficult to keep industry in any long-term sense from utilizing that technology. I think U.S. industry today does utilize the technology where it is not dealing with the Government.

Mr. CONYERS. Have you got a view on the FBI's proposed legislation that would prohibit using encryption technology in the United States?

Mr. SOCOLAR. Yes. It seems to me that it is the view of industry that the FBI's proposal will impede the development of digital communications technology and it will prohibit American businesses from securing their communications. They believe that if the system is open to FBI surveillance of the type that the Bureau is recommending, it would be vulnerable to the threat of foreign economic espionage agencies, organized crime, and even sophisticated hackers.

The telecommunications industry has demonstrated a willingness to work with the FBI to meet the FBI's needs in complying with

court-ordered wiretaps. I believe Director Sessions has testified in the past that the Bureau has not really run into any problems yet, and it therefore seems to me, again, without coming to any kind of a final conclusion on the question you ask, that too is a proper subject for congressional consideration in terms of the issues that are involved.

Mr. CONYERS. Thank you.

Finally, would you have gotten more information for this hearing if you hadn't been stiffed by the FBI and the CIA?

Mr. SOCLAR. We could have gotten more information of a detailed nature. The information that we got was generalized in recognition of the problem and also in recognition of the fact that it has been one of long standing, but we really were not able to get any of the kind of detail that would give us a better sense of just how deeply the issue really did go.

[Response to Mr. Brooks' questions for the record follow:]

MR. BROOKS' QUESTIONS FOR THE RECORD FOR MR. SOCOLAR

1. Please provide a more detailed summary of the Hitachi theft of IBM secrets and other espionage cases.

Response: In 1982, employees of Hitachi Ltd. of Tokyo pleaded guilty to conspiring to transport stolen IBM property--design documents and components for every major part of IBM's newest and most powerful generation of computers, not yet on the market. Hitachi, a Japanese manufacturer of IBM-compatible products, planned to use these items to eliminate costly and time-consuming reverse engineering, thereby shortening the lead time required to bring Hitachi products to the marketplace. In an elaborate sting operation that lasted several months, the FBI, working closely with IBM, recorded numerous episodes in which Hitachi employees conspired to buy proprietary IBM equipment and documents from undercover agents. Another Japanese company, Mitsubishi, also pleaded guilty to the theft of IBM secrets, as did employees of an American company involved in a joint development project with Hitachi. It is unclear whether the Japanese government was involved, because of the close relationship and inter-dependency between Japanese industry and the Japanese government. The companies involved in the theft paid IBM hundreds of millions of dollars to settle a civil law suit in this matter.

In another case, two men were arrested in a September 1978 sting operation for attempting to bribe the Administrator of Technology Exchange of Intel, Inc., to obtain the latest revision masks of computer memory chips for Intel's high speed computers. It was suspected that these men were agents of the Soviet Union. In 1979, Intel compared computer memory circuits from the Soviet Union and Japan (Toshiba) with its own and declared that they were direct copies of Intel memory boards.

In a third case, a top research scientist sold or attempted to sell trade secrets belonging to the Norton Company and General Electric to a South Korean company and a Chinese company. The trade secrets concerned the U.S. companies' processes for manufacturing high quality industrial diamonds that are used for drill bits and other equipment. U.S. intelligence agencies refused to tell us whether the scientist who sold the proprietary information had been recruited by a foreign intelligence agency.

2. Please describe the technical and policy problems with the FBI's "Digital Telephony" legislation.

Response: As I mentioned at the hearing, it is our understanding that the telecommunications industry is concerned that the FBI's proposed legislation may impede the development of advanced digital communications in the United States and may prevent American businesses from protecting their communications from the threat of economic espionage, organized crime, and even sophisticated hackers.

At the request of the Subcommittee on Telecommunications and Finance, House Committee on Energy and Commerce, GAO's Information Management and Technology Division is currently looking at the nature of the wiretapping technology problems. The result of this work will put us in a better position to discuss the information technology issues associated with the FBI's proposed legislation.

3. Please provide your views on the Digital Signature Standard and any problems associated with this proposed standard.

Response: The need for an internationally accepted digital signature standard arises from the increase in electronic commerce and communications. In the years to come, billions of electronic transactions will replace the traditional paper transactions of governments, industries, academia, and private citizens.

Certain electronic communications will be protected by techniques that enable parties receiving a communication to authenticate the identity of the sender by his or her unique "digital signature," in place of a traditional ink and paper signature. A digital signature also ensures integrity of the message. In addition, the algorithm, or mathematical procedure, that supports a digital signature may support privacy of messages.

The National Institute of Standards and Technology (NIST) proposed a U.S. standard for digital signature in August 1991¹ that provides sender verification and message integrity but not message privacy. If adopted, federal agencies, unless granted a waiver, will be required to use the NIST standard, as will industry when conducting business with the U.S. government.

We believe that adoption of NIST's standard would create problems for U.S. industry for many reasons. The NIST standard relies on an algorithm that does not comply with the international standard. A digital signature standard, commercially known as RSA² (ISO/IEC 9796³), is already generally accepted by the international community and by many in U.S. industry. RSA is the most widely used algorithm that complies with the international digital signature standard. The specifications of the international standard are based on the RSA algorithm. Many large U.S. software producers and other companies--such as IBM, Apple, Microsoft, Citicorp/Citibank, Motorola, Lotus Development Corporation,

¹Through a 1982 Federal Register notice (47 Fed. Reg. 28,445 1982), NIST requested alternative algorithms, or mathematical formulas, to be used for a digital signature standard. However, NIST abandoned this effort because of pressure from the National Security Agency.

²The acronym RSA stands for the last names of its inventors--Rivest, Shamir, and Adleman.

³International Organization for Standardization/International Electrotechnical Commission 9796, "Information Technology Security Techniques - Digital Signature Scheme Giving Message Recovery," ISO/IEC JTC1/SC27N289, July 18, 1991.

and Digital Equipment Corporation--are already using RSA or are producing or evaluating RSA-based software. Users of Internet, the world's largest data network, use RSA for privacy-enhanced electronic mail. If the proposed NIST standard is adopted, it appears that industry conducting business with the U.S. government and with international entities will have to use both standards, thereby increasing industry costs.

In addition, it appears that computer resource costs to support NIST's proposed standard would be higher than costs to support the use of the international standard, when considering the broad range of applications that will be used. The major reason for higher cost is that the digital signature standard algorithm is slower in signature verification--the most frequent, most time-consuming, and, therefore, most costly operation in the digital signature process.

Further, RSA, when used as the international standard, would provide greater assurance of protecting the authenticity of messages and signatures than would the NIST proposed standard for two reasons: the international standard permits a longer "key" length and RSA has been tested for about a decade. The proposed NIST standard requires that its key--conceptually, a string of numbers that must be guessed to forge the digital signature--be relatively short; and this may permit compromise of many senders' keys in 5 to 10 years. In addition, the NIST standard is based on an algorithm that has not been adequately tested by the international cryptographic community. Cryptographers require that an algorithm be thoroughly tested for many years before they are confident that it is adequate.

Also, the potential cost of royalties for using each standard must be considered. Although NIST intended to provide a royalty-free standard, royalties may have to be paid to the holders of patents relative to the proposed digital signature standard algorithm. While RSA is patented in the United States, the U.S. government's use of RSA would be royalty-free because it was developed, in part, with National Science Foundation funds.

Finally, NIST's proposed standard does not support confidential or private electronic messages. RSA does. The privacy of messages is normally achieved by using one other algorithm. In order to achieve privacy of messages with the proposed digital signature standard, two additional algorithms would be required. RSA requires only one additional algorithm, such as the Data Encryption Standard, to achieve privacy of messages.

A U.S. standard for digital signature, when selected, should be at least as effective--in terms of cost, performance, and security--as the international standard. Because of the lack of security assurances and the additional costs associated

with adoption of the proposed standard, we believe that NIST should reassess the merit of its proposed standard.

4. Is it within the mandate of the CIA and the FBI to protect industry from international economic espionage?

Response: Executive order 12333, which addresses U.S. intelligence activities, directs that "special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States government, or United States corporations, establishments, or persons." (Executive Order 12333, 1.1(c) (1981)).

Mr. CONYERS. Thank you very much.

The Chair recognizes the gentleman from Illinois, Mr. Hyde.

Mr. HYDE. Thank you very much, Mr. Chairman.

Mr. Socolar, you, I'm sure, understand the need for the FBI and the CIA to protect sources and methods. I mean that is a given, is it not?

Mr. SOCOLAR. Yes, I would agree with that.

Mr. HYDE. And it is not as if they are self-contained operations accountable to nobody. That is only independent counsel that has that Olympian status. They have to respond to the House Permanent Select Committee on Intelligence and the Senate Permanent Select Committee on Intelligence made up of Members of Congress and staff, and that structure is set up to protect sources and methods. At least that is the idea anyway. Whether it always works that way is another matter.

But I detect then some understanding and even some sympathy with the need for those agencies and other intelligence agencies to protect sources and methods.

Mr. SOCOLAR. Oh, yes, I fully agree with that. I think, though, that there is a range of information that could be provided that would give greater detail than we were able to get that could still be provided without jeopardizing sources and methods.

Mr. HYDE. That is always the big problem. It is one of judgment. Smart people can interpret and extrapolate from information much more than just the information that is given. You can make deductions if you are clever and you are able to fill in the background, and I suppose people of good will can argue over whether this information would not compromise sources and methods or whether it would.

But I am not as concerned with the reticence of those agencies so long as the same questions can be asked by other people in an environment that is more secure.

Mr. SOCOLAR. I agree. That is really where the dilemma lies in dealing with the subject matter that we are talking about here today. On the one hand, we have the need related to national security; we do have the need for a certain amount of secrecy; yet, at the same time, it seems to me that there are large public policy issues here as to exactly how this dilemma is going to be resolved, and that only comes about through an open debate of the policy issues, not so much even the specific detail.

Mr. HYDE. But the General Accounting Office is the investigative arm of the Congress, and in the areas of intelligence there are other structures established designed to protect sensitive information, and the Congress, I guess what I want to say, is not denied that information, it is just denied it through your agency when a dispute exists as to whether the information is of such a sensitive nature as to possibly compromise sources and methods, which I think may be a little cumbersome from your perspective, but we as a body, the legislative body, are not denied that information, we just have to go elsewhere to get it, I guess. That must be frustrating to you, but—

Mr. SOCOLAR. Well, actually, in doing this work, I wouldn't say that it was designed to come up with any kinds of definitive answers to these large questions. What we were interested in doing

in responding to the subcommittee's request was to pull together the kind of information that does exist to define the problem and to lay out the kinds of concerns that the Congress is, in fact, going to have to deal with, in my judgment.

Mr. HYDE. Thank you very much.

Mr. CONYERS. Thank you very much.

The Chair recognizes the distinguished gentleman from New York, Mr. Fish.

Mr. FISH. Thank you, Mr. Chairman.

Just as a footnote on this past colloquy, I have every confidence that should we desire more information from our intelligence community that it would be happy to come join us in executive session.

Mr. Socolar, I want to thank you for distilling, if I understand you correctly, the issues here as to the extent to which U.S. intelligence should be assisting U.S. business, and, second, the extent to which U.S. business should be denied the most advanced technology to protect its proprietary data.

With that in mind, going back generally here, how complicated is it to determine whether a particular instance of espionage is being conducted by a foreign government as distinct from a foreign company—what do you look at to make a determination?

Mr. SOCOLAR. Ultimately it has to be determined on the basis of investigation and determinations as to what relationship whoever has stolen the information can be traced to his or her government. I don't think that that shows up on the surface; that only gets determined after a thorough investigation.

Mr. FISH. I should imagine there would be an added difficulty with what you refer to as government-to-industry relationships with respect to Japan, which of course has a substantially different arrangement than enjoyed in this country.

What other countries in your experience have this government-to-industry relationship?

Mr. SOCOLAR. Well, obviously the former Soviet Union has that kind of a relationship. The two that come to mind for me are Japan and the Soviet Union.

Mr. FISH. All right. Starting on page 5, we get into the question of the cryptographic and other information technologies, and that is readily available, but the intelligence community appears to be insisting on the development of a different standard that is weaker, and I don't think anybody has asked especially why. Why are they doing that?

Mr. SOCOLAR. I can only surmise with regard to that question. Apparently, to the extent that this advanced technology is disseminated, that, in itself, limits the ability of our own intelligence agencies to monitor electronic transmissions.

Mr. FISH. You mean to say, what would be a greater protection for the proprietary data for industry handicaps the intelligence agencies from monitoring?

Mr. SOCOLAR. That is correct. That really is at the heart of one of the dilemmas in the situation.

Mr. FISH. Thank you.

Finally, you say in your testimony on page 6 that, in your judgment, the CIA and the FBI do not appear to be sufficiently coordinated to adequately protect U.S. industry against economic espionage.

nage. Could you give us the basis for your conclusion and your recommendations on how this coordination can be improved.

Mr. SOCOLAR. Well, I think the basis for that statement really lies in what we have been talking about in terms of the controversy that exists over phone technology, over the cryptographic standards for U.S. companies, in terms of how our intelligence agencies are dealing with those issues.

Mr. FISH. Do you have any suggestions, Mr. Socolar, as to how the coordination could be improved?

Mr. SOCOLAR. The only suggestion I would be able to make would be one that I would have to repeat, and that is that it is important to have these issues debated, dealt with, and arrive at a consensus that would have the intelligence communities and the Department of Commerce, in connection with sensitive, unclassified information, moving in the same directions.

Mr. FISH. Thank you very much.

Mr. CONYERS. Thank you, Mr. Fish.

The Chair recognizes the gentleman from Kentucky, Mr. Mazzoli.

Mr. MAZZOLI. Thank you very much, Mr. Chairman.

I'm not sure if this suggests that great minds run in the same path, but the two areas that I had looked to get into were the two that my friend from New York got into, so let me go back at those again, Mr. Socolar.

On page 5 of your testimony, you quote Mr. Gates. He is here, and he will decide whether that is an accurate quotation or taken out of context. But, I gather you use that to under-gird your case for saying that neither the CIA nor the FBI, nor the NSA are in a position to help American industry.

Mr. SOCOLAR. No. I don't use it for that purpose. I use it essentially to point out where the intelligence community appears to be on the issue.

Mr. MAZZOLI. If I understand it correctly, what this quotation suggests, and, what you say is the truth, is that the intelligence agencies of the country do not want to get into economic espionage. Is that the case?

Mr. SOCOLAR. That is my understanding, yes.

Mr. MAZZOLI. What is your understanding of economic espionage?

Mr. SOCOLAR. Economic espionage, to me, is essentially the theft of information from the United States, from U.S. companies, by foreign governments.

Mr. MAZZOLI. The CIA would not be into economic espionage. They would be stealing from whom and for what purpose?

Mr. SOCOLAR. I think the question would be whether the CIA should be stealing foreign companies' secrets.

Mr. MAZZOLI. So, in other words, you understand economic espionage to be stealing from U.S. companies, but the CIA's situation was with regard to their stealing from foreign companies. Is that correct?

Mr. SOCOLAR. That is correct.

Mr. MAZZOLI. And you suggest that because they are not able to get into economic espionage, that American companies are left on the market either to use existing highly sophisticated technology which could provide problems to our intelligence agencies or, conversely, to use a lesser standard, which I want to hear about later

on, which then would provide no problem to the intelligence agencies but could provide no great protection for American companies. Is that your understanding of the issue?

Mr. SOCOLAR. That is correct.

Mr. MAZZOLI. So we have to decide whether or not this so-called lesser technology is, in fact, capable of protecting American companies from espionage directed against them. Now if I understand correctly, it is from somewhere else against them to secure economic information which could be advantageous to a competitor or to another country or whatever else. Is that correct?

Mr. SOCOLAR. That is correct.

Mr. MAZZOLI. Have you reached a conclusion as to whether or not this new technology is, in fact, disabling or helping American companies?

Mr. SOCOLAR. Well, U.S. industry is very clear, it seems to me—

Mr. MAZZOLI. I didn't ask that question, sir. I asked whether the GAO has reached an opinion.

Mr. SOCOLAR. Yes. From our analysis, I would say that the technology that the Department of Commerce is proposing is a much weaker technology for the protection of electronic transmission and is also, I might say, an added burden to U.S. industry, because the advanced technology is out there for U.S. industry to use, it can freely use it, and this would require a separate technology for U.S. industry in dealing with the U.S. Government.

Mr. MAZZOLI. OK. Just out of curiosity, is that study available? Is it a lengthy study? Could a nonscientist like the questioner understand any part of it?

Mr. SOCOLAR. We can make available to you the basis for that conclusion.

Mr. MAZZOLI. Well, make it to the committee. And, one further question, was this information that you have examined or was regurgitated by the industry, or was it done independently by GAO?

[See Mr. Socolar's response to Chairman Brooks' questions for the record, p. 22.]

Mr. SOCOLAR. This was information that we received from industry but also was analyzed within GAO in terms of the strength of the standard.

Mr. MAZZOLI. OK. And you mention here "Such technology"—meaning the higher, advanced new generation—"Such technology is readily available under internationally accepted industry standards." "Readily available"? I mean where do you buy that, in Zurich, or do you buy it in New York? Where do you buy that stuff?

Mr. SOCOLAR. It is purchased from companies in the United States—Digital Equipment Corp., Lotus.

Mr. MAZZOLI. So if I understand correctly, at some point this committee will be asked by agencies of Government to disallow American companies from buying equipment which is being sold here in the United States to protect themselves? Is that your understanding of what will be asked of this committee?

Mr. SOCOLAR. Yes. For certain purposes, industry will be required to use a standard other than the one that is highly protective and freely available.

Mr. MAZZOLI. A standard other than the one highly protective implies that the other standard is not one which would highly protect. That is still your conclusion?

Mr. SOCOLAR. That is right. It is referred to as a digital signature standard that is being proposed by the Department of Commerce.

Mr. MAZZOLI. Thank you.

I would have one last inquiry, and that is, again, the question of the so-called cooperation or, as you say, sufficiently coordinated to adequately protect because we have already read—in the statement of the CIA—that it does not get into aggressive international economic espionage. But, now you are saying here that you concluded that they cannot protect U.S. companies. Is it because that is not their role, or they cannot handle that role, or they are just not equipped to do it, or don't want to do it, or what?

Mr. SOCOLAR. It is because they are not assuming that role—not that they cannot, but that they will not.

Mr. MAZZOLI. But if they were to assume it, do you think they could fulfill it?

Mr. SOCOLAR. I think it is like all other intelligence activities; they will meet with success to a certain degree, but they will not catch all of it.

Mr. MAZZOLI. Is there anything to your knowledge—my last question—that would prevent the CIA or FBI from accepting such a role? Is that within their mandate?

Mr. SOCOLAR. I would have to give you an answer for the record on that.

Mr. MAZZOLI. I appreciate that. Thank you very much.

[See Mr. Socolar's responses to Chairman Brooks' questions for the record, p. 22.]

Mr. MAZZOLI. Thank you, Mr. Chairman.

Mr. BROOKS [presiding]. Thank you very much, Mr. Socolar, gentlemen, ladies.

Mr. JAMES. Mr. Chairman.

Mr. BROOKS. Mr. James has not been recognized?

Mr. JAMES. Not yet, Mr. Chairman.

Mr. BROOKS. And Lamar Smith has not been recognized?

We have got two witnesses waiting, and I sure hope we will not take a lot of time.

Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Socolar, a couple of very brief questions. In response a while ago to your definition of "economic espionage," you considered it to be the theft of American technology by a foreign government. You didn't specifically include foreign companies. Is that a distinction without a difference, or is it all the same to you?

Mr. SOCOLAR. No. I think there is a difference there. I think company to company is really within the framework of old-fashioned competition, I suppose.

Mr. SMITH. If there is a distinction there, to what extent is each guilty of economic espionage? Do you see the primary perpetrators of theft of technology to be governments or to be foreign companies that are not acting under the auspices of their governments?

Mr. SOCOLAR. I have no way of quantifying that. I think both go on. There is certainly company-to-company theft of proprietary information right here in the United States.

Mr. SMITH. In regard to your comments concerning the FBI and the CIA, I feel that you see it as primarily a problem of enforcement, not one of laws. Leaving aside the enforcement for a minute because we are going to be hearing from representatives of those organizations, do you see any laws that Congress should consider that would help reduce the problem?

Mr. SOCOLAR. I haven't made a thorough study of the statutes that are on the books as affected by this particular problem. My general impression, though, is that there need to be some laws enacted defining the kinds of theft that occur here that really don't come under—

Mr. SMITH. So far you have been concentrating on the enforcement side. So you think there does need to be congressional action as far as new laws are concerned as well.

Mr. SOCOLAR. That is correct.

Mr. SMITH. OK. For the record, if you will, give us some details as to the nature of those laws that you feel should be addressed. Thank you.

Mr. SOCOLAR. I would be happy to, yes.

[The information was provided directly to Mr. Smith.]

Mr. SMITH. Thank you, Mr. Chairman.

Mr. BROOKS. Thank you.

Mr. James, the gentleman from Florida.

Mr. JAMES. Thank you.

Mr. Socolar, I was reading the examples that IBM submitted in their statement, as on page 3 where Recon Optical, Inc., a U.S. company, contracted with the Israeli Government to design a top secret airborne spy camera system. After months of disagreement, Israel apparently, it was alleged, turned it over to one of their contractors and thereby entered into competition. The other example they gave was the French allegedly were involved in misappropriations of proprietary information from two U.S. companies; they give an example there.

My question is, it seems to me that it would be more in the nature of the laws and the remedy within the courts—in other words, if there's a cause of action and if you can find jurisdiction and you can get your defendant in the proper jurisdiction, you can file a suit. Otherwise, the private company would be out of luck.

To what extent and how would the CIA or the FBI involvement change this, in other words? You still would have to deal with whatever the existing legal structure was, isn't that correct, as a remedy?

Mr. SOCOLAR. Certainly a lot of these thefts are subject to suit in the courts. One problem is, though, that companies very often have no way of knowing whether they've been victimized by this kind of—

Mr. JAMES. These aren't good examples, then, of what we're really talking about, economic espionage, because it is very obvious that what happened was after the fact as the product appeared on the market. I assume, too, you would have enforcement within certain trade agreements and the Department of Commerce or who-

ever, the United States, could respond appropriately alleging a breach of trade agreements; that's another area, once you find out the information.

Mr. SOCOLAR. There is another example of why it's important to review the statutes as to what kinds of prosecutions are available.

Mr. JAMES. So we're not talking about changing laws; we're talking about trying to collect information so that the companies will be in a position to make a determination as to enforcement or the United States will be in a position to make a determination as to what they should do in relationship to the trade agreements.

I can see an agency being involved in order to protect the United States. What I question is, to what extent do we use either the FBI or the CIA as an investigator, if you will—because that's all it amounts to, because you're dependent upon whatever laws we have passed—what we're saying, then, is that we're going to let certain private companies have the benefits, I suppose, with some vague standard as to what constitutes economic espionage. We're going to fund, through taxpayers' money, a private investigator to collect information to protect American corporations; is that what it's all about?

Do you understand the spirit of my question or what I'm asking?

Mr. SOCOLAR. Yes, I do. But as I would characterize the issue, it's whether our intelligence agencies should be using their resources to seek technological, proprietary information, to be of assistance to U.S. companies in the interest of the extent to which the economic well-being of our country is related to its national security also.

Mr. JAMES. In other words, if we're to draw a law—if we're to consider this issue, we would have to draw parameters for when, in fact, will we use the investigative arm of either agency for the purposes of assisting a U.S. company. Do you have any suggestion as to how we would approach that?

Mr. SOCOLAR. No. As I said earlier, the only suggestion I have is to be thinking about it, to be debating it, and to ultimately come to a conclusion that arises out of that.

Mr. JAMES. Thank you so much.

Mr. BROOKS. Thank you very much.

Thank you very much, Mr. Socolar.

Mr. SOCOLAR. Thank you.

Mr. BROOKS. And Mr. Podell, Mr. Burke, and Ms. Stewart-Murray.

Our second panel is comprised of highly distinguished Federal Government officials. We want to welcome a fellow Texan and FBI Director William S. Sessions, as he makes his first appearance before the Economic and Commercial Law Subcommittee. Judge Sessions received his undergraduate and law degrees from Baylor University in Waco, subsequently practicing law there. He was appointed U.S. district judge for the Western District of Texas in 1974 and became Chief Judge of that court in 1980, where he served until he became FBI Director in November 1987.

We also want to especially welcome CIA Director Robert M. Gates, who appears before the Judiciary Committee for the first time in a public, open meeting. That's a new openness program down at the CIA. He began his career at the CIA in 1966, and from

1974 to 1979, he was assigned to the National Security Council staff. He was appointed to other administrative positions prior to his return to the CIA in 1982. He became Director of Central Intelligence in November 1991.

Our final witness on this panel is Dr. James J. Hearn, Deputy Director for Information Systems Security at the National Security Agency. Prior to his civilian service, Dr. Hearn was a naval officer assigned to the Naval Propulsion Headquarters engineering staff. He began his career at the National Security Agency in 1964—the year Lyndon Johnson was reelected—as a design engineer and has held his current position since August 1988.

Gentlemen, I appreciate your being here. We will proceed under the same guidelines as before. We hope you will make a short statement. Your written statements will be put in the record in full, and any additions or questions we might submit, we will submit some of them possibly to you. Otherwise, we will ask you those questions if we have the time. We have one more panel so we're not going to take much more of your time. You've already had about an hour and a half of sitting around.

Judge, you may proceed.

STATEMENT OF WILLIAM S. SESSIONS, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. SESSIONS. Mr. Chairman, I greatly appreciate the opportunity to be here. I would ask that, if there are questions relating to Mr. Socolar's testimony that relate to the FBI, with its relationship with the CIA and with its counterintelligence responsibility, that I be allowed to respond for the record to a number of those points that he raised which I believe are, at best, superficial, and certainly do not show a deep knowledge of the relationship between the FBI and the CIA in its counterintelligence efforts. I would like to respond to those, if I may, if they don't come up in questioning.

Mr. BROOKS. All right. Without objection.

Mr. SESSIONS. Mr. Chairman, I am very pleased to appear and address the important and timely issue of economic espionage. As the committee is aware, during the past 3 years, revolutionary changes across that part of the world that was formerly known as the Soviet bloc of nations have been tremendous. The world has watched intensely as momentous events have reshaped the political and economic landscape of the Soviet Union and Eastern Europe. The collapse of various Communist parties and Marxist doctrines created an environment where repressed peoples began to experience political and personal freedom, to plan for market economies, and to envision new societies built on traditions of humanism and enlightenment.

The FBI views these recent changes with a great deal of optimism. However, one cannot ignore the fact that these transitions have met with opposition and difficulties, as evidenced by political and economic turmoil, as well as ethnic tensions across that entire region.

In view of the changing world order, I wish that I could say that there is no longer an intelligence threat against the United States. To do so would be grossly inaccurate. While the focus may be changing, clearly the intelligence threat remains. It is a threat that

remains remarkably consistent from traditional collectors, but that no longer can be defined solely in terms of the military concern that a particular government poses to the United States.

The traditional domination of most East European intelligence services by the Soviet Intelligence Service has ended. Eastern European nations are restructuring their intelligence services to serve their own interests. The extent of change and the pace of this restructuring varies significantly from country to country. We must recognize that the foreign intelligence threat is no longer confined to those foreign powers which are historically antagonistic to our national objectives.

As in the past, many countries are targeting their intelligence collectors against the United States in operations which extend far beyond obtaining information for traditional defense needs. Now and in the future, the collection strategies of adversaries and allies alike will not only focus on defense-related information but also include scientific, technological, political, and economic information. This type of intelligence will be critical for building modern, market-oriented systems that will be capable of competing on an international scale.

I will take out that part of my statement that relates to information that was testified to previously.

In a recent article by Chairman McCurdy of the House Permanent Select Committee on Intelligence, the chairman stated, "As the European market unifies late in 1992, we may see a much more aggressive effort by some countries to protect their industrial base by targeting American competitors as sources of valuable data that can be used to enhance their own products and marketing strategies. Hence, we must have a robust counterintelligence program to thwart such activities."

Likewise, on the Senate side, Chairman David Boren has stated, "Direct theft of American private secrets by foreign government intelligence services is not yet a massive undertaking. But as we go into the next century, and as international relations become much more a matter of economic competition than military competition, it's going to really increase."

I believe that they're correct and that the FBI must be prepared to meet these new challenges.

I will now focus for a moment on the concept of economic espionage and the FBI's role in dealing with this issue now and in the future.

As you well know, Mr. Chairman, on an annual basis, the U.S. Government publicly issues the National Security Strategy of the United States. This document, signed by the President, sets forth the broad goals, objectives, interests, and direction that provide definition to the effort to protect our Nation's national security. Included within the definition of this strategy is the protection of the traditional classified information, as well as the protection of proprietary economic and technical information belonging to U.S. corporations.

Mr. BROOKS. Judge, would the gentleman yield just a moment?

Mr. SESSIONS. I certainly will.

[Whereupon, the subcommittee proceeded to other business.]

Mr. BROOKS. The hearing is now back in order.

Judge, we will recognize you now to continue.

Mr. SESSIONS. As I was stating, included within the definition of the strategy is the protection of the traditional classified information, as well as the protection of proprietary economic and technical information belonging to U.S. corporations.

In response to a changing world and these concerns, the FBI has moved steadily, since 1989, to bring about a significant revamping of our approach to conducting counterintelligence investigations. This was to ensure that the FBI fulfills our mandate and our responsibilities under the National Security Strategy.

On February 1 of this year, and in accordance with Attorney General guidelines for conducting foreign counterintelligence investigations, the FBI implemented what we call the national security threat list approach to safeguarding our national security in the face of a rapidly changing threat. This dramatically, as I characterize it, forward-thinking counterintelligence investigative strategy is intended to frustrate intelligence activities that threaten the U.S. national security both from the traditional side as well as from the nontraditional side, and it includes economic espionage concerns.

It is independent of but works in conjunction with FBI jurisdiction exercised over the widely divergent existing criminal statutes, the violations of which are investigated by the FBI, of course, in their responsibility. This new strategy does not revolve solely around particular countries and their political positions in the world.

The national security threat list approach also addresses certain "issue threats." These are foreign intelligence activities directed against specifically identified U.S. individuals or entities which, if compromised, would be detrimental to the U.S. national security. So, for the purpose of today's hearing, the two most relevant issues on the list are foreign intelligence activities directed at critical or core technologies in the United States, and foreign intelligence activities directed at the collection of proprietary economic information and technologies.

I will forgo what I have on the next several pages—that is, a listing of those kinds of technologies which we have at issue.

Proprietary technology and economic information are more difficult to define and includes information concerning unclassified U.S. business and economic resources, activities, research and development, and policies. While unclassified, the loss of this information could adversely impact on the ability of the United States to compete in the world marketplace, and its loss would have been and will continue to have a detrimental affect on the U.S. economy, ultimately—and I underscore the word "ultimately"—weakening national security.

Protection of this type of information is the most difficult aspect of implementing our national security threat list program. While the administration and the U.S. intelligence community recognize that protecting proprietary economic information is necessary to maintain the competitiveness of the United States in the international marketplace, the intelligence community, as well as the business community, have not yet agreed on a clear definition of proprietary information.

Perhaps just as critical as classified and technological information is the need to protect information on corporate negotiating positions, costs, economic feasibility studies, and marketing plans. These confidential corporate trade secrets or reports can more directly affect the competitive position of U.S. firms possibly than the firm's technology.

One of the major difficulties with this issue is the protection of unclassified information. Business leaders and the intelligence community are attempting to clearly define this issue to determine what information and technology needs to be encompassed. In the interim, the FBI is investigating alleged attempts by foreign government entities and intelligence services to collect proprietary technology and economic information that are essential to our national security.

Under this counterintelligence program and the national security threat list concept, the FBI does not investigate corporate theft of technology or information by competitive firms; that is, activity that is not State sponsored. However, this type of activity sometimes involves a violation of Federal criminal statutes and FBI investigations have in the past resulted in prosecutions, of which you're all aware.

The FBI's criminal jurisdiction, both domestically and internationally, is clear. Under existing criminal statutes, however, the FBI has only a limited ability to counter the unfair economic advantage of foreign businesses and industry which often is fostered by foreign governments and their intelligence services. The anti-trust laws, the antidumping provisions, certain tariff and trade reciprocal actions, and economic enforcement provisions are all available to the Government to improve our competitive position. Additionally, clear lines are also drawn with respect to violations involving patents, copyrights, trademarks, and the interstate transportation of stolen property.

Liaison with other Federal agencies has always been an important aspect of foreign counterintelligence. Although the FBI is the lead agency for counterintelligence matters in the United States, other agencies have criminal responsibilities that intersect our own, particularly in reference to issue threats. The U.S. Customs Service, for example, has primary responsibility under the Arms Export Act to investigate violations of the U.S. Department of State munitions list, and under the Export Administration Act for foreign investigation of dual-use items. Customs also shares responsibility for domestic investigation with the Department of Commerce, and has primary responsibility under the Trading with the Enemy Act and the International Emergency Economic Power Act to control items embargoed or sanctioned by the Office of Foreign Assets Control. Perhaps the most uncertain area involves that of intellectual property and trade secrets. These types of information appear to fall within an area that is not clearly defined, either from a criminal or a counterintelligence perspective.

Mr. Chairman, I commend you and the committee for your interest and concern regarding this important issue. The changing world political situation and the globalization of what used to be local economies makes these issues even more critical. The FBI, as you well know, has significant responsibilities, both from the coun-

terintelligence and criminal standpoints, and undoubtedly will play a significant role in helping the United States deal with these issues.

Our criminal jurisdiction is broad and strongly encompasses both domestic and international activity that violates Federal criminal laws. On the counterintelligence side, I am particularly proud that the FBI anticipated the changing circumstances and revamped our counterintelligence strategies to meet these new challenges. As the Congress tackles these tough issues, I am confident that you will find the FBI is fully prepared to meet our responsibilities under those statutes.

Thank you, sir.

Mr. BROOKS. Thank you, Judge.

[The prepared statement of Mr. Sessions follows:]

**PREPARED STATEMENT OF WILLIAM S. SESSIONS, DIRECTOR, FEDERAL
BUREAU OF INVESTIGATION**

THANK YOU MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE. I AM PLEASED TO APPEAR BEFORE YOU TO ADDRESS THE IMPORTANT AND TIMELY ISSUE OF ECONOMIC ESPIONAGE. AS THE COMMITTEE IS AWARE, DURING THE PAST THREE YEARS, REVOLUTIONARY CHANGES HAVE SWEEPED ACROSS WHAT WE FORMERLY KNEW AS THE SOVIET BLOC OF NATIONS. THE WORLD HAS WATCHED INTENSELY AS MOMENTOUS EVENTS HAVE RESHAPED THE POLITICAL AND ECONOMIC LANDSCAPE OF THE SOVIET UNION AND EASTERN EUROPE. THE COLLAPSE OF VARIOUS COMMUNIST PARTIES AND MARXIST DOCTRINES CREATED AN ENVIRONMENT WHERE REPRESSED PEOPLES BEGAN TO EXPERIENCE POLITICAL AND PERSONAL FREEDOM, TO PLAN FOR MARKET ECONOMIES, AND TO ENVISION NEW SOCIETIES BUILT ON TRADITIONS OF HUMANISM AND ENLIGHTENMENT. IT WOULD HAVE BEEN UNIMAGINABLE THREE YEARS AGO THAT I WOULD BE MEETING WITH RUSSIAN OFFICIALS IN MY OFFICE AT FBI HEADQUARTERS, BUT THIS HAS HAPPENED. IT WOULD HAVE BEEN INCONCEIVABLE TO THINK THAT THE FBI DIRECTOR WOULD TRAVEL TO POLAND TO EXPLORE WITH POLISH OFFICIALS WAYS IN WHICH THE FBI CAN ASSIST IN ESTABLISHING "THE RULE OF LAW"

THROUGH INTERNATIONAL POLICE TRAINING. THIS TOO HAS COME TO PASS. THESE ARE INDEED HISTORIC TIMES. THE FBI VIEWS THESE RECENT CHANGES WITH A GREAT DEAL OF OPTIMISM. HOWEVER, ONE CANNOT IGNORE THE FACT THAT THESE TRANSITIONS HAVE MET WITH OPPOSITION AND DIFFICULTIES AS EVIDENCED BY POLITICAL AND ECONOMIC TURMOIL, AS WELL AS ETHNIC TENSIONS ACROSS THE REGION. LEADERS IN THOSE CHANGING GOVERNMENTS ARE NOW FORCED TO DEAL WITH AN INCREASINGLY MOBILE POPULATION AND WITH DILEMMAS THAT HAVE NO PRECEDENT. AS THESE NATIONS MOVE TO MORE FREELY INTERACT WITH THE WEST, UNITED STATES FOREIGN POLICY HAS MOVED FROM A POSITION OF CONTAINMENT OF COMMUNISM TO ONE OF GREATER ENGAGEMENT WITH OPENNESS AND EXCHANGES WITH THESE EMERGING DEMOCRACIES.

SURROUNDED BY THIS "AIR OF OPTIMISM" AND IN VIEW OF THE CHANGING WORLD ORDER, I WISH THAT I COULD SAY THAT THERE IS NO LONGER AN INTELLIGENCE THREAT AGAINST THE UNITED STATES. TO DO SO WOULD BE GROSSLY INACCURATE. WHILE THE FOCUS MAY BE CHANGING, CLEARLY THE INTELLIGENCE THREAT REMAINS. IT IS A THREAT THAT REMAINS REMARKABLY

CONSISTENT FROM TRADITIONAL COLLECTORS, BUT THAT NO LONGER CAN BE DEFINED SOLELY IN TERMS OF THE MILITARY CONCERN A PARTICULAR GOVERNMENT POSES TO THE UNITED STATES. THE TRADITIONAL DOMINATION OF MOST EAST EUROPEAN INTELLIGENCE SERVICES BY THE SOVIET INTELLIGENCE SERVICE HAS ENDED. EAST EUROPEAN NATIONS ARE RESTRUCTURING THEIR INTELLIGENCE SERVICES TO SERVE THEIR OWN INTERESTS. THE EXTENT OF CHANGE AND THE PACE OF THIS RESTRUCTURING VARIES SIGNIFICANTLY FROM COUNTRY TO COUNTRY. WE MUST RECOGNIZE THAT THE FOREIGN INTELLIGENCE THREAT IS NOT CONFINED TO THOSE FOREIGN POWERS WHICH ARE HISTORICALLY ANTAGONISTIC TO OUR NATIONAL OBJECTIVES. AS IN THE PAST, MANY COUNTRIES ARE TARGETING THEIR INTELLIGENCE COLLECTORS AGAINST THE UNITED STATES IN OPERATIONS WHICH EXTEND FAR BEYOND OBTAINING INFORMATION FOR TRADITIONAL DEFENSE NEEDS. NOW AND IN THE FUTURE, THE COLLECTION STRATEGIES OF ADVERSARIES AND ALLIES ALIKE WILL NOT ONLY FOCUS ON DEFENSE RELATED INFORMATION, BUT ALSO INCLUDE SCIENTIFIC, TECHNOLOGICAL, POLITICAL AND ECONOMIC INFORMATION. THIS TYPE OF INTELLIGENCE WILL BE CRITICAL FOR

BUILDING MODERN MARKET-ORIENTED ECONOMIC SYSTEMS THAT WILL BE CAPABLE OF COMPETING ON AN INTERNATIONAL SCALE.

DEFECTORS FROM THE FORMER SOVIET UNION AND NEWLY INDEPENDENT RUSSIA HAVE OPENLY PREDICTED THAT THE NEW INDEPENDENT STATES WILL ESCALATE INDUSTRIAL ESPIONAGE ACTIVITIES IN THE YEARS AHEAD TO BOLSTER THEIR ECONOMIES AND FOSTER INCREASED TECHNOLOGICAL PROGRESS. DEFECTORS HAVE STATED THAT THE NEW RUSSIAN INTELLIGENCE SERVICE WILL TARGET THE INCREASING NUMBER OF U.S./RUSSIAN JOINT BUSINESS VENTURES IN AN EFFORT TO STEAL HIGHLY DESIRABLE WESTERN TECHNOLOGY. ACCORDING TO MANY SOURCES, RUSSIANS DO NOT HAVE THE CURRENCY TO PAY FOR ADVANCE BUSINESS SYSTEMS AND DESIGNS SO THEY WILL STEAL THEM OR OBTAIN THEM THROUGH OTHER ILLEGITIMATE MEANS. I BELIEVE THAT THE COMMITTEE IS AWARE OF COMMENTS LAST SEPTEMBER BY PIERRE MARION, THE RETIRED HEAD OF THE FRENCH EXTERNAL INTELLIGENCE SERVICE DURING A U.S. TELEVISION INTERVIEW. ON THE NBC BROADCAST "EXPOSÉ," HE STATED THAT THE FRENCH GOVERNMENT DID NOT HESITATE TO TARGET UNITED STATES ECONOMIC AND PROPRIETARY INFORMATION BECAUSE, "IN

ECONOMIC MATTERS, WE ARE NOT ALLIED." HE DETAILED HOW U.S. BUSINESSMEN WERE TARGETED BY THE FRENCH SERVICE. OTHER FOREIGN NATIONS LIKEWISE ARE ECONOMICALLY MOTIVATED TO COLLECT CLASSIFIED AND UNCLASSIFIED SCIENTIFIC AND TECHNOLOGICAL INFORMATION BECAUSE THE TREND OF TECHNOLOGICAL "PROTECTIONISM" IN LEADING ECONOMIC COUNTRIES HAS MADE THE DESIRE TO ATTAIN THE SAME TECHNOLOGICAL LEVEL AS THAT OF MORE ADVANCED NATIONS MORE URGENT.

IN A RECENT ARTICLE BY CHAIRMAN MCCURDY OF THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, THE CHAIRMAN STATED, "AS THE EUROPEAN MARKET UNIFIES BEGINNING IN LATE 1992, WE MAY SEE A MUCH MORE AGGRESSIVE EFFORT BY SOME COUNTRIES TO PROTECT THEIR INDUSTRIAL BASE BY TARGETING AMERICAN COMPETITORS AS SOURCES OF VALUABLE DATA THAT CAN BE USED TO ENHANCE THEIR OWN PRODUCTS AND MARKETING STRATEGIES ... HENCE, WE MUST HAVE A ROBUST COUNTERINTELLIGENCE PROGRAM TO THWART SUCH ACTIVITIES." LIKEWISE, ON THE SENATE SIDE, CHAIRMAN DAVID BOREN HAS STATED "DIRECT THEFT OF AMERICAN PRIVATE

SECRETS BY FOREIGN GOVERNMENT INTELLIGENCE SERVICES IS NOT YET A MASSIVE UNDERTAKING. BUT AS WE GO INTO THE NEXT CENTURY, AND AS INTERNATIONAL RELATIONS BECOME MUCH MORE A MATTER OF ECONOMIC COMPETITION THAN MILITARY COMPETITION ... IT'S GOING TO REALLY INCREASE." I BELIEVE THAT THEY ARE CORRECT AND THAT THE FBI MUST BE FULLY PREPARED TO MEET THESE NEW CHALLENGES.

I WOULD LIKE TO FOCUS ON THE CONCEPT OF "ECONOMIC ESPIONAGE" AND THE FBI'S CHALLENGING ROLE IN DEALING WITH THIS ISSUE NOW AND IN THE FUTURE. ON AN ANNUAL BASIS, THE UNITED STATES GOVERNMENT PUBLICLY ISSUES THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES. THIS DOCUMENT, SIGNED BY THE PRESIDENT, SETS FORTH THE BROAD GOALS, OBJECTIVES, INTERESTS AND DIRECTION THAT PROVIDE DEFINITION TO THE EFFORT TO PROTECT OUR NATION'S NATIONAL SECURITY. INCLUDED WITHIN THE DEFINITION OF THIS STRATEGY IS THE PROTECTION OF TRADITIONAL CLASSIFIED INFORMATION AS WELL AS THE PROTECTION OF PROPRIETARY ECONOMIC AND TECHNICAL INFORMATION BELONGING TO U.S. CORPORATIONS. IN RESPONSE TO A

CHANGING WORLD AND THESE CONCERNS, THE FBI HAS MOVED STEADILY SINCE 1989 TO BRING ABOUT A SIGNIFICANT REVAMPING IN OUR APPROACH TO CONDUCTING COUNTERINTELLIGENCE INVESTIGATIONS. THIS WAS TO ENSURE THAT THE FBI FULFILLS OUR MANDATE AND OUR RESPONSIBILITIES UNDER THE NATIONAL SECURITY STRATEGY. ON FEBRUARY 1ST OF THIS YEAR, AND IN ACCORDANCE WITH ATTORNEY GENERAL GUIDELINES FOR CONDUCTING FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS, THE FBI IMPLEMENTED WHAT WE CALL THE NATIONAL SECURITY THREAT LIST APPROACH TO SAFEGUARDING OUR NATIONAL SECURITY IN THE FACE OF A RAPIDLY CHANGING THREAT. THIS DRAMATICALLY FORWARD THINKING COUNTERINTELLIGENCE INVESTIGATIVE STRATEGY IS INTENDED TO FRUSTRATE INTELLIGENCE ACTIVITIES THAT THREATEN UNITED STATES NATIONAL SECURITY BOTH FROM THE TRADITIONAL SIDE AS WELL AS THE NON-TRADITIONAL SIDE AND INCLUDES ECONOMIC ESPIONAGE CONCERNS. IT IS INDEPENDENT OF, BUT WORKS IN CONJUNCTION WITH, FBI JURISDICTION EXERCISED OVER THE WIDELY DIVERGENT EXISTING CRIMINAL STATUTES, THE VIOLATIONS OF WHICH ARE INVESTIGATED BY THE FBI. THIS NEW STRATEGY

DOES NOT REVOLVE SOLELY AROUND PARTICULAR COUNTRIES AND THEIR POLITICAL POSITIONS IN THE WORLD. THE NATIONAL SECURITY THREAT LIST APPROACH ALSO ADDRESSES CERTAIN "ISSUE THREATS." THESE ARE FOREIGN INTELLIGENCE ACTIVITIES DIRECTED AGAINST SPECIFICALLY IDENTIFIED U.S. INDIVIDUALS OR ENTITIES WHICH, IF COMPROMISED, WOULD BE DETRIMENTAL TO UNITED STATES NATIONAL SECURITY. FOR THE PURPOSE OF TODAY'S HEARING, THE TWO MOST RELEVANT ISSUES ON THIS LIST ARE: (1) FOREIGN INTELLIGENCE ACTIVITIES DIRECTED AT CRITICAL OR "CORE" TECHNOLOGIES IN THE UNITED STATES AND (2) FOREIGN INTELLIGENCE ACTIVITIES DIRECTED AT THE COLLECTION OF PROPRIETARY ECONOMIC INFORMATION AND TECHNOLOGY IN THE UNITED STATES.

CRITICAL TECHNOLOGIES, SOMETIMES REFERRED TO AS CORE TECHNOLOGIES OR NATIONAL CRITICAL TECHNOLOGIES, IS AN ISSUE THAT HAS BEEN EXTENSIVELY DEBATED IN THE NATIONAL SECURITY POLICY COMMUNITY. CRITICAL TECHNOLOGIES ARE DIVIDED INTO THREE CATEGORIES. NATIONAL CRITICAL TECHNOLOGIES ARE IDENTIFIED AS TECHNOLOGIES DEEMED CRITICAL TO ENHANCE NATIONAL SECURITY AND ECONOMIC

COMPETITIVENESS. EXAMPLES OF NATIONAL CRITICAL TECHNOLOGIES INCLUDE MANUFACTURING PROCESSES AND TECHNOLOGIES, INFORMATION AND COMMUNICATIONS TECHNOLOGIES, AERONAUTICS AND SURFACE TRANSPORTATION SYSTEMS, AND ENERGY AND ENVIRONMENT RELATED TECHNOLOGIES. DEPARTMENT OF DEFENSE CRITICAL TECHNOLOGIES FOCUS EXCLUSIVELY ON TECHNOLOGIES THAT ARE ESSENTIAL TO MAINTAIN THE QUALITATIVE SUPERIORITY OF U.S. WEAPONS SYSTEMS. SEMICONDUCTOR MATERIALS AND MICROELECTRIC CIRCUITS, SOFTWARE ENGINEERING, HIGH PERFORMANCE COMPUTING, SIMULATION MODELING, SENSITIVE RADAR AND SUPERCONDUCTIVITY ARE A FEW EXAMPLES. IN THE SPRING OF 1990, THE DEPARTMENT OF COMMERCE IDENTIFIED SEVERAL EMERGING TECHNOLOGIES WHICH ARE EXPECTED TO HAVE THE POTENTIAL OF CONTRIBUTING TO THE DEVELOPMENT OF NEW IMPROVED PRODUCTS BY THE YEAR 2000. THESE MOSTLY UNCLASSIFIED TECHNOLOGIES FALL UNDER THE PROPRIETARY ECONOMIC INFORMATION AND TECHNOLOGY ISSUE. EXAMPLES OF THESE TECHNOLOGIES ARE COMPUTER SOFTWARE, COMPUTER-INTEGRATED MANUFACTURING AND CERTAIN MEDICAL

TECHNOLOGIES. ALL OF THE ABOVE TECHNOLOGIES REQUIRE A CONCENTRATED EFFORT OF PROTECTION FROM FOREIGN POWERS TO PRESERVE THE ECONOMIC VITALITY OF THIS COUNTRY AND ENSURE THE CONTINUED COMPETITIVENESS OF THE UNITED STATES IN THE INTERNATIONAL MARKETPLACE.

PROPRIETARY TECHNOLOGY AND ECONOMIC INFORMATION IS MORE DIFFICULT TO DEFINE AND INCLUDES "INFORMATION CONCERNING UNCLASSIFIED U.S. BUSINESS AND ECONOMIC RESOURCES, ACTIVITIES, RESEARCH AND DEVELOPMENT, AND POLICIES." WHILE UNCLASSIFIED, THE LOSS OF THIS INFORMATION COULD ADVERSELY IMPACT ON THE ABILITY OF THE UNITED STATES TO COMPETE IN THE WORLD MARKETPLACE, AND ITS LOSS WOULD HAVE A DETRIMENTAL AFFECT ON THE UNITED STATES ECONOMY, ULTIMATELY WEAKENING NATIONAL SECURITY. PROTECTION OF THIS TYPE OF INFORMATION IS THE MOST DIFFICULT ASPECT OF IMPLEMENTING OUR NATIONAL SECURITY THREAT LIST PROGRAM. WHILE THE ADMINISTRATION AND THE UNITED STATES INTELLIGENCE COMMUNITY RECOGNIZE THAT PROTECTING PROPRIETARY ECONOMIC INFORMATION IS NECESSARY TO MAINTAIN THE COMPETITIVENESS OF THE UNITED

STATES IN THE INTERNATIONAL MARKETPLACE, THE INTELLIGENCE COMMUNITY AS WELL AS THE BUSINESS COMMUNITY HAVE NOT YET AGREED ON A CLEAR DEFINITION OF PROPRIETARY INFORMATION. PERHAPS JUST AS CRITICAL AS CLASSIFIED AND TECHNOLOGICAL INFORMATION IS THE NEED TO PROTECT CORPORATE NEGOTIATING POSITIONS, COSTS, ECONOMIC FEASIBILITY STUDIES AND MARKETING PLANS. THESE CONFIDENTIAL CORPORATE "TRADE SECRETS" OR REPORTS CAN MORE DIRECTLY AFFECT THE COMPETITIVE POSITION OF U.S. FIRMS THAN THE FIRM'S TECHNOLOGY. ONE OF THE MAJOR DIFFICULTIES WITH THIS ISSUE IS THE PROTECTION OF UNCLASSIFIED INFORMATION. BUSINESS LEADERS AND THE INTELLIGENCE COMMUNITY ARE ATTEMPTING TO CLEARLY DEFINE THIS ISSUE TO DETERMINE WHAT INFORMATION AND TECHNOLOGY NEEDS TO BE ENCOMPASSED. IN THE INTERIM, THE FBI IS INVESTIGATING ALLEGED ATTEMPTS BY FOREIGN GOVERNMENT ENTITIES AND INTELLIGENCE SERVICES TO COLLECT PROPRIETARY TECHNOLOGY AND ECONOMIC INFORMATION THAT ARE ESSENTIAL TO NATIONAL SECURITY. UNDER THE COUNTERINTELLIGENCE PROGRAM AND THE NATIONAL SECURITY THREAT LIST CONCEPT, THE FBI DOES NOT INVESTIGATE

CORPORATE THEFT OF TECHNOLOGY OR INFORMATION BY COMPETITOR FIRMS, THAT IS, ACTIVITY THAT IS NOT STATE SPONSORED. HOWEVER, THIS TYPE OF ACTIVITY SOMETIMES INVOLVES A VIOLATION OF FEDERAL CRIMINAL STATUTES AND FBI INVESTIGATIONS HAVE IN THE PAST RESULTED IN PROSECUTIONS.

THE FBI'S CRIMINAL JURISDICTION BOTH DOMESTICALLY AND INTERNATIONALLY IS CLEAR. UNDER EXISTING CRIMINAL STATUTES, HOWEVER, THE FBI HAS ONLY A LIMITED ABILITY TO COUNTER THE UNFAIR ECONOMIC ADVANTAGE OF FOREIGN BUSINESSES AND INDUSTRY WHICH OFTEN IS FOSTERED BY FOREIGN GOVERNMENTS AND THEIR INTELLIGENCE SERVICES. THE ANTI-TRUST LAWS, THE ANTI-DUMPING PROVISIONS, CERTAIN TARIFF AND TRADE RECIPROCAL ACTIONS AND ECONOMIC ENFORCEMENT PROVISIONS ARE ALL AVAILABLE TO GOVERNMENT TO IMPROVE OUR COMPETITIVE POSITION. ADDITIONALLY, CLEAR LINES ARE ALSO DRAWN WITH RESPECT TO VIOLATIONS INVOLVING PATENTS, COPYRIGHTS, TRADEMARKS AND THE INTERSTATE TRANSPORTATION OF STOLEN PROPERTY. LIAISON WITH OTHER FEDERAL AGENCIES HAS ALWAYS BEEN AN IMPORTANT ASPECT OF FOREIGN COUNTERINTELLIGENCE. ALTHOUGH THE FBI IS THE LEAD

AGENCY FOR COUNTERINTELLIGENCE MATTERS IN THE UNITED STATES, OTHER AGENCIES HAVE CRIMINAL RESPONSIBILITIES THAT INTERSECT OUR OWN, PARTICULARLY IN REFERENCE TO ISSUE THREATS. THE U.S. CUSTOMS SERVICE FOR EXAMPLE, HAS PRIMARY RESPONSIBILITY UNDER THE ARMS EXPORT CONTROL ACT TO INVESTIGATE VIOLATIONS OF THE U.S. DEPARTMENT OF STATE MUNITIONS LIST; AND UNDER THE EXPORT ADMINISTRATION ACT FOR FOREIGN INVESTIGATION OF "DUAL USE" ITEMS. CUSTOMS SHARES RESPONSIBILITY FOR DOMESTIC INVESTIGATION WITH THE DEPARTMENT OF COMMERCE; AND HAS PRIMARY RESPONSIBILITY UNDER THE TRADING WITH THE ENEMY ACT AND INTERNATIONAL EMERGENCY ECONOMIC POWER ACT TO CONTROL ITEMS EMBARGOED OR SANCTIONED BY THE OFFICE OF FOREIGN ASSETS CONTROL. PERHAPS THE MOST UNCERTAIN AREA INVOLVES THAT OF INTELLECTUAL PROPERTY AND TRADE SECRETS. THESE TYPES OF INFORMATION APPEAR TO FALL WITHIN AN AREA THAT IS NOT CLEARLY DEFINED, EITHER FROM A CRIMINAL OR A COUNTERINTELLIGENCE PERSPECTIVE.

MR. CHAIRMAN, I COMMEND YOU AND THE COMMITTEE FOR YOUR INTEREST AND CONCERN REGARDING THIS IMPORTANT

ISSUE. THE CHANGING WORLD POLITICAL SITUATION AND THE GLOBALIZATION OF WHAT USED TO BE LOCAL ECONOMIES MAKES THESE ISSUES EVEN MORE CRITICAL. THE FBI HAS SIGNIFICANT RESPONSIBILITIES BOTH FROM THE COUNTERINTELLIGENCE AND CRIMINAL STANDPOINTS AND UNDOUBTEDLY WILL PLAY A SIGNIFICANT ROLE IN HELPING THE UNITED STATES DEAL WITH THESE ISSUES. OUR CRIMINAL JURISDICTION IS BROAD AND STRONGLY ENCOMPASSES BOTH DOMESTIC AND INTERNATIONAL ACTIVITY THAT VIOLATES FEDERAL CRIMINAL LAWS. ON THE COUNTERINTELLIGENCE SIDE I AM PROUD THAT THE FBI ANTICIPATED CHANGING CIRCUMSTANCES AND REVAMPED OUR COUNTERINTELLIGENCE STRATEGIES TO MEET THESE NEW CHALLENGES. AS CONGRESS TACKLES THESE TOUGH ISSUES, I AM CONFIDENT YOU WILL FIND THE FBI FULLY PREPARED TO MEET OUR RESPONSIBILITIES.

Mr. BROOKS. Director Gates.

STATEMENT OF ROBERT M. GATES, DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Mr. GATES. Thank you, Mr. Chairman. As you requested, Mr. Chairman, I will summarize my statement and the full statement can go in the record.

Monitoring foreign intelligence activity against U.S. economic interests is part of our broader responsibility in the intelligence community for tracking global developments that affect American economic competitiveness. One of our tasks in the economic area is to undertake counterintelligence measures, as necessary, to protect our economy from those who do not play by the rules.

Let me emphasize here that the CIA does not, and will not, engage in commercial espionage. We do not penetrate foreign companies for the purpose of collecting business information of interest to U.S. corporations. In our view, it is the role of U.S. business to size up foreign competitors' trade secrets, market strategies, and bid proposals. But we do operate overseas to monitor foreign government sponsored targeting of American businesses.

Various governments in Asia, Europe, the Middle East, and to a lesser degree, Latin America, as well as some former Communist countries—some 20 countries or governments in all—are involved in intelligence activities that are detrimental to our economic interests at some level.

In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world are shifting the emphasis in targeting. Foreign targeting of American technology continues. Some foreign governments target a range of economic and business data. They want access to U.S. Government policy deliberations concerning foreign trade, investments, loans, and positions on bilateral economic negotiations. Several governments also seek information about company bids for contracts, information that affects prices of commodities, financial data, and banking information affecting stock market trends and interest rates.

The number of foreign intelligence services capable of conducting sophisticated operations has increased. There has been a proliferation of commercially available intelligence technologies. A number of Third World intelligence services, over 50, in fact, have profited from training they received in the past from East bloc services.

There are many gradations in the threat. In assessing what sort of threat various activities constitute, we look at several basic questions. First, who is conducting the activity. Often, the primary actor from a given country is not an intelligence organization but a business or another component of the government performing de facto intelligence functions, such as a trade organization or economics ministry.

Second, we look at what is being collected, the shopping list. This may be embargoed technology or classified research. Much valuable information is available also from open sources.

Third, we look at where the information is obtained. Most services are most aggressive against U.S. targets inside their own coun-

tries where they can control the operating environment better and the legal environment is naturally benign.

Fourth, we consider how the information is acquired. In human operations, some intelligence services that stop short of recruiting U.S. citizens use intelligence operatives to elicit information from them. Another tactic employed has been to use local employees of U.S. subsidiaries overseas to collect information.

A number of services conduct technical operations against U.S. businesses. On the low tech end, such things as bugging hotel rooms of traveling American executives occurs. We also operate on the assumption that any technically sophisticated intelligence service could mount a technical attack against U.S. businesses or businessmen in those countries.

Finally, we look at why the information is collected and what is done with it. A number of countries disseminate economic information and some economic intelligence to individual national firms.

We can discern several distinct collection patterns, each more or less characteristic of one or more countries today. The first pattern is classic espionage, in which a foreign intelligence organization operates clandestinely on a global basis to recruit and run paid agents in U.S. companies and governmental institutions.

In the second pattern, an intelligence organization relies largely on elicitation rather than outright recruitment.

Third, the intelligence service operates "bag operations" within its own border, surreptitiously entering hotel rooms of visiting American officials or executives to search for documents containing sensitive economic or business data.

Fourth, the government operates not through intelligence services per se but through other components to conduct an extensive, systematic program of collecting information of economic value—largely from open sources—and disseminating it to business leaders.

The fifth pattern, a government covertly targets sensitive weapons technology by working through front organizations, military attachés, and special intelligence units that operate outside of regular intelligence organizations. And an emerging sixth pattern is that of intelligence entrepreneurs prepared to sell their services either to foreign governments or to private organizations.

Let me conclude by saying what we do with the information. First, we provide information and analysis of foreign economic intelligence collection to policymakers. Second, we provide detailed counterintelligence briefings to contractors working on classified projects for the intelligence community, the CIA. Third, in coordination with the FBI, we inform an individual company if we detect an intelligence operation directed specifically against it overseas. In all such cases, we take care to protect sources and methods. This sometimes requires that the information we provide be in a generic fashion, but we usually find a way to tell the company what it needs to know to take corrective action.

Fourth, we maintain close liaison with other U.S. Government agencies. If we come across information that does not fall within our purview, we pass it to the appropriate department.

Mr. Chairman, I will conclude my abbreviated statement at that point. Thank you.

Mr. BROOKS. Thank you very much.
[The prepared statement of Mr. Gates follows:]

PREPARED STATEMENT OF ROBERT M. GATES, DIRECTOR, CENTRAL
INTELLIGENCE AGENCY

INTRODUCTION. MR. CHAIRMAN, I AM
HERE TODAY IN RESPONSE TO YOUR REQUEST
THAT I ADDRESS THE PROBLEM OF FOREIGN
ECONOMIC ESPIONAGE AND OTHER DESTRUCTIVE
ACTIVITIES THAT ADVERSELY AFFECT OUR
ECONOMIC VIGOR. THIS IS AN IMPORTANT
SUBJECT THAT WE IN THE INTELLIGENCE
COMMUNITY TAKE VERY SERIOUSLY.
MONITORING FOREIGN INTELLIGENCE ACTIVITY
AGAINST US ECONOMIC INTERESTS IS PART OF
OUR BROADER RESPONSIBILITY FOR TRACKING
GLOBAL DEVELOPMENTS THAT AFFECT AMERICAN
ECONOMIC COMPETITIVENESS. FOREIGN
ECONOMIC INTELLIGENCE COLLECTION IS BY
NO MEANS A NEW ISSUE FOR THE
INTELLIGENCE COMMUNITY, BUT IT IS ONE
THAT IS ASSUMING EVEN GREATER IMPORTANCE
THAN PREVIOUSLY. THE MOST FAR-REACHING
REVIEW OF NATIONAL INTELLIGENCE NEEDS
SINCE 1947 WAS UNDER-TAKEN LAST YEAR,
WITH SOME TWENTY POLICY AGENCIES AND
DEPARTMENTS PARTICIPATING. THE
RESULTING NATIONAL SECURITY REVIEW,
SIGNED BY THE PRESIDENT ON NOVEMBER
15TH, HIGHLIGHTED INTERNATIONAL ECONOMIC

TRENDS AS A PRIORITY INTELLIGENCE ISSUE. NEARLY FORTY PERCENT OF THE REQUIREMENTS IN THE DIRECTIVE ARE ECONOMIC IN NATURE, REFLECTING THE REALIZATION OF SENIOR POLICYMAKERS THAT MANY OF THE MOST IMPORTANT CHALLENGES AHEAD ARE IN THE INTERNATIONAL ECONOMIC ARENA.

ESSENTIALLY, CIA HAS THREE BROAD TASKS WITH RESPECT TO ECONOMIC ISSUES.

-- THE FIRST IS TO SUPPORT US POLICYMAKERS IN THE EXECUTIVE AND LEGISLATURE BRANCHES AS THEY SET THIS COUNTRY'S ECONOMIC POLICY COURSE--BY PROVIDING THEM WITH ASSESSMENTS ABOUT BROAD ECONOMIC FORCES AND TRENDS AND THE CULTURAL FACTORS THAT INFLUENCE THEM.

-- THE SECOND TASK IS TO MONITOR TRENDS IN TECHNOLOGY THAT COULD AFFECT NATIONAL SECURITY. WE

MUST WATCH CLOSELY THE DEVELOPMENT OF FOREIGN CAPABILITIES IN ADVANCED TECHNOLOGICAL AREAS--BY NO MEANS SOLELY MILITARY--THAT PROMISE TO HAVE MAJOR SECURITY AND ECONOMIC IMPACTS.

-- THE THIRD TASK IS TO UNDERTAKE COUNTERINTELLIGENCE MEASURES AS NECESSARY TO PROTECT OUR ECONOMY FROM THOSE WHO DO NOT PLAY BY THE RULES. LET ME EMPHASIZE HERE THAT CIA DOES NOT AND WILL NOT ENGAGE IN COMMERCIAL ESPIONAGE. WE DO NOT PENETRATE FOREIGN COMPANIES FOR THE PURPOSE OF COLLECTING BUSINESS INFORMATION OF INTEREST TO US CORPORATIONS. IT IS THE ROLE OF US BUSINESS TO SIZE UP FOREIGN COMPETITORS' TRADE SECRETS, MARKET STRATEGIES, AND BID PROPOSALS. BUT WE DO OPERATE

OVERSEAS TO MONITOR FOREIGN
GOVERNMENT-SPONSORED TARGETING OF
AMERICAN BUSINESSES.

MY COMMENTS TODAY WILL NOT DEAL COMPREHENSIVELY WITH THE FULL RANGE OF PRACTICES EMPLOYED BY FOREIGN GOVERNMENTS AND COMPANIES TO GAIN ADVANTAGE IN COMPETING WITH US BUSINESS, OR THEIR USE OF VARIOUS LEGAL MECHANISMS TO GAIN ACCESS TO US RESEARCH. INSTEAD, I WILL CONCENTRATE LARGELY ON FOREIGN INTELLIGENCE COLLECTION THAT THREATENS OUR ECONOMIC INTERESTS. I HOPE I CAN PROVIDE A SENSE OF THE SCOPE AND CHARACTER OF THE PROBLEM. OBVIOUSLY, IN AN OPEN HEARING I CANNOT DISCUSS THE PROBLEM IN DETAIL OR REFER TO PARTICULAR COUNTRIES. I CAN NOTE, HOWEVER, THAT SOME GOVERNMENTS IN ASIA, EUROPE, THE MIDDLE EAST, AND TO A LESSER DEGREE LATIN AMERICA, AS WELL AS SOME FORMER COMMUNIST COUNTRIES--NEARLY 20 GOVERNMENTS OVERALL--ARE INVOLVED IN INTELLIGENCE COLLECTION ACTIVITIES THAT

ARE DETRIMENTAL TO OUR ECONOMIC INTERESTS AT SOME LEVEL.

THE CHANGING THREAT. OUR FUNDAMENTAL ASSESSMENT IS THAT WHILE THE END OF THE COLD WAR DID NOT BRING AN END TO THE FOREIGN INTELLIGENCE THREAT, IT DID CHANGE THE NATURE OF THAT THREAT. THE THREAT HAS BECOME MORE DIVERSIFIED AND MORE COMPLEX. IN A WORLD THAT INCREASINGLY MEASURES NATIONAL POWER AND NATIONAL SECURITY IN ECONOMIC TERMS AS WELL AS MILITARY TERMS, MANY FOREIGN INTELLIGENCE SERVICES AROUND THE WORLD ARE SHIFTING THE EMPHASIS IN TARGETING. FOREIGN TARGETING OF AMERICAN TECHNOLOGY CONTINUES; TECHNOLOGY IS IMPORTANT FOR ECONOMIC AS WELL AS MILITARY REASONS. SINCE THE US CONTINUES TO BE ON THE CUTTING EDGE OF TECHNOLOGICAL INNOVATION, TECHNOLOGY THEFT WILL REMAIN A MAJOR CONCERN FOR US.

BUT SOME FOREIGN INTELLIGENCE OPERATIONS AGAINST OUR ECONOMIC INTERESTS ENCOMPASS MORE THAN TECHNOLOGY DIVERSION. SOME FOREIGN GOVERNMENTS

TARGET A RANGE OF ECONOMIC AND BUSINESS DATA. THEY WANT ACCESS TO US GOVERNMENT POLICY DELIBERATIONS CONCERNING FOREIGN TRADE, INVESTMENTS, AND LOANS, AND POSITIONS ON BILATERAL ECONOMIC NEGOTIATIONS. SEVERAL GOVERNMENTS ALSO SEEK INFORMATION ABOUT COMPANY BIDS FOR CONTRACTS, INFORMATION THAT AFFECTS PRICES OF COMMODITIES, FINANCIAL DATA, AND BANKING INFORMATION AFFECTING STOCK MARKET TRENDS AND INTEREST RATES.

IN ADDITION TO COLLECTING ECONOMIC INFORMATION, SOME FOREIGN INTELLIGENCE SERVICES HAVE TRIED TO EXERT CLANDESTINE INFLUENCE ON US BUSINESS AND GOVERNMENT DECISIONS THAT AFFECT THEIR ECONOMIC INTERESTS--BY ATTEMPTING TO RECRUIT AGENTS OF INFLUENCE IN US GOVERNMENT, BANKING, AND BUSINESS CIRCLES. WE KNOW ONE COUNTRY THAT HAS RECENTLY BEEN PUSHING SUCH SO-CALLED "ACTIVE MEASURES" IN THE ECONOMIC AREA. SEVERAL OTHER GOVERNMENTS ENGAGE IN AGGRESSIVE LOBBYING ON BEHALF OF THEIR NATIONAL FIRMS--TO THE POINT OF EXERTING

POLITICAL AND ECONOMIC LEVERAGE IN A HEAVY-HANDED MANNER.

ANOTHER REASON THE THREAT HAS BECOME MORE DIFFUSE IN RECENT YEARS IS THAT THE NUMBER OF FOREIGN INTELLIGENCE SERVICES CAPABLE OF CONDUCTING SOPHISTICATED OPERATIONS HAS INCREASED. THERE HAS BEEN A PROLIFERATION OF COMMERCIALY AVAILABLE INTELLIGENCE TECHNOLOGIES. IN ADDITION TO TECHNOLOGIES FOR INTELLIGENCE OPERATIONS BECOMING CHEAPER, A NUMBER OF THIRD WORLD INTELLIGENCE SERVICES--OVER 50, IN FACT--HAVE PROFITED FROM TRAINING THEY RECEIVED IN THE PAST FROM EAST BLOC SERVICES, AND THEY ARE NOW MORE ABLE TO ACT UNILATERALLY. AT THE SAME TIME, WITH LARGE NUMBERS OF INTELLIGENCE OPERATIVES THROWN OUT OF THEIR JOBS IN SOME FORMER COMMUNIST COUNTRIES, THE RESERVOIR OF PROFESSIONALLY TRAINED INTELLIGENCE MERCENARIES IS GROWING.

IN AN ENVIRONMENT OF HEIGHTENED GLOBAL ECONOMIC AND TECHNOLOGICAL COMPETITION, AND ONE IN WHICH

INTELLIGENCE CAPABILITIES HAVE PROLIFERATED, THE DANGER EXISTS OF INTELLIGENCE OPERATIONS BEING CONDUCTED AGAINST OUR ECONOMIC INTERESTS FROM A VARIETY OF SOURCES. FIRST OF ALL, THOSE OF OUR TRADITIONAL ADVERSARIES THAT REMAIN IN BUSINESS AGAINST US ARE GIVING A HIGH PRIORITY TO BOTH TECHNOLOGY THEFT AND ECONOMIC INTELLIGENCE COLLECTION. THIS IS TRUE OF INTELLIGENCE SERVICES BOTH IN UNREFORMED COMMUNIST COUNTRIES AND IN SOME REFORMING FORMER COMMUNIST COUNTRIES. THE ECONOMIC DISTRESS THAT FORMER COMMUNIST COUNTRIES ARE EXPERIENCING IN SOME CASES GIVES IMPETUS TO INTELLIGENCE EFFORTS TO ACQUIRE INFORMATION AND ADVANCED TECHNOLOGY OF COMMERCIAL VALUE TO THEM. THE COMMUNIST GOVERNMENTS THAT REMAIN, FEELING INCREASINGLY ISOLATED AND THREATENED BY "DEMOCRATIC ENCIRCLEMENT," CONTINUES TO VIEW TECHNOLOGY THEFT AS ONE MEANS OF PROPPING UP THEIR REPRESSIVE REGIMES, MILITARY ARSENALS, AND SAGGING ECONOMIES.

FOR MANY COUNTRIES, COLLECTION OF WEAPONS TECHNOLOGY SERVES BOTH ECONOMIC AND MILITARY ENDS. THE TECHNOLOGY MAY ENHANCE THE COUNTRY'S MILITARY CAPABILITIES, WHILE ALSO MAKING ITS ARMAMENTS INDUSTRIES BETTER ABLE TO COMPETE WITH US SUPPLIERS IN INTERNATIONAL ARMS MARKETS. THE EXTREMELY SENSITIVE NATURE OF THE INFORMATION PERTAINING TO WEAPONS PROLIFERATION--CHEMICAL, BIOLOGICAL, NUCLEAR, AND BALLISTIC MISSILES--HAS LED GOVERNMENTS INTERESTED IN PROCURING WEAPONS TECHNOLOGY TO LEAN HEAVILY ON THEIR INTELLIGENCE SERVICES.

WE ALSO HAVE TO BE WATCHFUL OF THE ACTIVITIES OF ADVANCED INDUSTRIAL COUNTRIES. SOME COUNTRIES WITH WHOM WE HAVE HAD GOOD RELATIONS MAY ADOPT A TWO-TRACK APPROACH OF COOPERATING WITH US AT THE LEVEL OF DIPLOMACY WHILE ENGAGING IN ADVERSARIAL INTELLIGENCE COLLECTION. AT PRESENT WE LACK THE EVIDENTIARY BASIS FOR ESTABLISHING ANY OVERALL TREND TOWARD INCREASED ECONOMIC ESPIONAGE AMONG ADVANCED INDUSTRIAL COUNTRIES.

NEVERTHELESS, ECONOMIC INTELLIGENCE COLLECTION BY SUCH COUNTRIES IS POTENTIALLY DAMAGING TO OUR ECONOMY BECAUSE THEY ARE STRONG ECONOMIC COMPETITORS, WHICH THE FORMER COMMUNIST STATES CLEARLY ARE NOT.

FINALLY, THERE IS A CATEGORY OF COUNTRIES THAT ARE NOT MAJOR ECONOMIC COMPETITORS OF THE US ACROSS THE BOARD BUT ARE COMPETITORS IN PARTICULAR SECTORS. COLLECTION OF ECONOMIC INTELLIGENCE BY SUCH COUNTRIES COULD DAMAGE THOSE PARTICULAR SECTORS OF THE US ECONOMY.

APPROACHING THE PROBLEM. CLEARLY, THERE ARE MANY GRADATIONS IN THE THREAT. FOREIGN EFFORTS TO GAIN ECONOMIC ADVANTAGE THROUGH COLLECTION PROGRAMS RUN THE GAMUT. SOME POSE SERIOUS PROBLEMS FOR THE US; OTHERS DO LITTLE DAMAGE. IN ASSESSING WHAT SORT OF THREAT VARIOUS ACTIVITIES CONSTITUTE, WE LOOK AT SEVERAL BASIC QUESTIONS.

FIRST, WHO IS CONDUCTING THE ACTIVITY? OFTEN THE PRIMARY ACTOR FROM A GIVEN COUNTRY IS NOT AN INTELLIGENCE ORGANIZATION BUT A BUSINESS OR ANOTHER COMPONENT OF THE GOVERNMENT PERFORMING DE FACTO INTELLIGENCE FUNCTIONS--SUCH AS A TRADE ORGANIZATION OR ECONOMICS MINISTRY. WHEN PRIVATE FIRMS ARE INVOLVED, AN INTELLIGENCE AGENCY OR GOVERNMENT IS SOMETIMES SPONSORING, ORCHESTRATING, OR COORDINATING THE ACTIVITY. THIS IS MORE LIKELY TO BE THE CASE IN COUNTRIES WITH CENTRALIZED ECONOMIES OR CORPORATIVE STRUCTURES IN WHICH THERE IS NO CLEAR SEPARATION BETWEEN PUBLIC AND PRIVATE SECTORS, BETWEEN BUSINESS COMPANIES AND GOVERNMENT AGENCIES.

TAKE, FOR EXAMPLE, THE CASE OF A SCIENTIST FROM A FOREIGN PRIVATE RESEARCH INSTITUTION WHO ATTENDS A PROFESSIONAL CONFERENCE IN THE US AND PICKS UP INFORMATION FROM COLLEAGUES IN OPEN DISCUSSION. WE CONSIDER WHETHER THE SCIENTIST IS A COOPTEE OF AN INTELLIGENCE SERVICE, WHETHER HE WAS

GIVEN COLLECTION REQUIREMENTS, WHETHER HE HAD AN OBLIGATION TO REPORT BACK TO HIS GOVERNMENT, AND WHETHER HIS TRIP WAS PART OF A SYSTEMATIC COLLECTION PROGRAM. ONE OR MORE OF THESE CIRCUMSTANCES MAY OBTAIN. A NUMBER OF MIDDLE EASTERN INTELLIGENCE SERVICES ARE ESPECIALLY ACTIVE IN USING SCIENTISTS TO COLLECT INFORMATION. (SIMILARLY, FOREIGN GOVERNMENTS SOMETIMES PLAY A ROLE BEHIND THE SCENES IN FACILITATING VISITS OF RESEARCHERS WORKING FOR FOREIGN CORPORATIONS TO OUR FEDERAL LABORATORIES OR ENCOURAGING FOREIGN BUSINESSES TO SPONSOR R&D PROGRAMS AT AMERICAN UNIVERSITIES THAT PROVIDE THEM SOME DEGREE OF PROPRIETARY CONTROL OVER THE TECHNOLOGY--THROUGH PATENTS OR LICENSES).

SECOND, WE LOOK AT WHAT IS BEING COLLECTED--THE "SHOPPING LIST," THIS MAY BE EMBARGOED TECHNOLOGY OR CLASSIFIED RESEARCH. BUT IT IS IMPORTANT TO KEEP IN MIND THAT MUCH VALUABLE INFORMATION IS AVAILABLE FROM OPEN SOURCES. EVEN MOST INTELLIGENCE

SERVICES--INCLUDING THOSE IN FORMER COMMUNIST COUNTRIES--HAVE BEGUN TO PLACE A HIGHER PREMIUM ON OPEN SOURCE COLLECTION. THIS IS PARTLY BECAUSE ADVANCES IN DATA PROCESSING HAVE MADE IT MUCH EASIER TO AGGREGATE, MANIPULATE, AND EXPLOIT LARGE VOLUMES OF DATA; IT IS PARTLY BECAUSE OPEN SOURCE COLLECTION IS LESS POLITICALLY RISKY FOR SERVICES THAT DO NOT WANT TO GET CAUGHT IN CLASSIC ESPIONAGE OPERATIONS.

THIRD, WE LOOK AT WHERE THE INFORMATION IS OBTAINED. FOREIGN INTELLIGENCE SERVICES ARE MORE INCLINED TO OPERATE AGAINST AMERICAN TARGETS OUTSIDE THE US. THEY KNOW THERE IS A GREATER CHANCE AMERICAN OFFICIALS WILL DETECT AN OPERATION TAKING PLACE ON OUR OWN TERRITORY, AND A GREATER LIKELIHOOD OF SERIOUS REPERCUSSIONS ONCE THE OPERATION IS DETECTED. MOST SERVICES ARE CONSEQUENTLY MORE AGGRESSIVE INSIDE THEIR OWN COUNTRIES, WHERE THEY CAN CONTROL THE OPERATING ENVIRONMENT BETTER AND THE LEGAL ENVIRONMENT IS NATURALLY BENIGN. OPERATIONS AGAINST US TARGETS

IN THIRD COUNTRIES CONSTITUTE ANOTHER APPROACH IN USE--ESPECIALLY BY SOME COMMUNIST AND FORMER COMMUNIST COUNTRIES.

FOURTH, WE CONSIDER HOW THE INFORMATION IS ACQUIRED. IN HUMAN OPERATIONS, SOME INTELLIGENCE SERVICES THAT STOP SHORT OF RECRUITING US CITIZENS USE INTELLIGENCE OPERATIVES TO ELICIT INFORMATION FROM THEM; THE TARGETED AMERICAN IS UNWITTING OF HIS INTERLOCUTOR'S INTELLIGENCE CONNECTION. ANOTHER TACTIC EMPLOYED HAS BEEN TO USE LOCAL EMPLOYEES OF US SUBSIDIARIES OVERSEAS TO COLLECT INFORMATION--JUST AS FOREIGN NATIONALS WORKING IN SUPPORT JOBS AT US EMBASSIES ARE SOMETIMES PRESSURED INTO REPORTING TO LOCAL COUNTERINTELLIGENCE SERVICES.

IN ADDITION TO HUMAN OPERATIONS, WE KNOW THAT A NUMBER OF SERVICES CONDUCT TECHNICAL OPERATIONS AGAINST US BUSINESSES. ON THE LOW TECH END, SUCH THINGS AS BUGGING HOTEL ROOMS OF TRAVELING AMERICAN EXECUTIVES OCCUR.

BEYOND SUCH PRACTICES, WE OPERATE ON THE ASSUMPTION THAT ANY TECHNICALLY SOPHISTICATED INTELLIGENCE SERVICE COULD MOUNT A TECHNICAL ATTACK AGAINST US BUSINESSES OR BUSINESSMEN IN THEIR COUNTRIES. ATTRACTIVE TARGETS WOULD BE A COMPANY'S COMMUNICATIONS AND COMPUTER SYSTEMS.

FINALLY, WE LOOK AT WHY THE INFORMATION IS COLLECTED AND WHAT IS DONE WITH IT. A NUMBER OF COUNTRIES, FOR EXAMPLE, DISSEMINATE ECONOMIC INFORMATION AND SOME ECONOMIC INTELLIGENCE TO INDIVIDUAL NATIONAL FIRMS. THIS PROCESS IS SOMETIMES REGULARIZED, BUT IS OFTEN ALSO FACILITATED BY THE EXISTENCE OF INFORMAL CHANNELS BETWEEN GOVERNMENT AND INDUSTRY.

PATTERNS OF ACTIVITY.

DISTINGUISHING BETWEEN THESE VARIOUS TYPES OF ACTIVITY, WE CAN DISCERN SEVERAL DISTINCT COLLECTION PATTERNS, EACH MORE OR LESS CHARACTERISTIC OF ONE OR MORE COUNTRIES TODAY.

THE FIRST PATTERN--MOST TYPICAL OF COMMUNIST COUNTRIES--IS CLASSIC ESPIONAGE, IN WHICH A FOREIGN INTELLIGENCE ORGANIZATION OPERATES CLANDESTINELY ON A GLOBAL BASIS TO RECRUIT AND RUN PAID AGENTS IN US COMPANIES AND GOVERNMENTAL INSTITUTIONS. THIS IS OFTEN DONE BY USING ACADEMIC, BUSINESS OR INTERNATIONAL ORGANIZATION COVER, WHICH OFTEN SUCCEED WHERE A STRAIGHTFORWARD PITCH TO WORK FOR A FOREIGN INTELLIGENCE SERVICE WOULD FAIL.

IN THE SECOND PATTERN, AN INTELLIGENCE ORGANIZATION RELIES LARGELY ON ELICITATION RATHER THAN OUTRIGHT RECRUITMENT.

IN THE THIRD PATTERN, THE INTELLIGENCE SERVICE CONDUCTS "BAG OPERATIONS" WITHIN ITS OWN BORDER, SURREPTITIOUSLY ENTERING HOTEL ROOMS OF VISITING AMERICAN OFFICIALS OR EXECUTIVES TO SEARCH FOR DOCUMENTS CONTAINING SENSITIVE ECONOMIC OR BUSINESS DATA, TAKING ADVANTAGE OF OTHER

SECURITY LAPSES AS WELL, AND PASSING THE INFORMATION GATHERED TO NATIONAL FIRMS.

IN THE FOURTH PATTERN, THE GOVERNMENT OPERATES NOT THROUGH INTELLIGENCE SERVICES PER SE BUT THROUGH OTHER COMPONENTS TO CONDUCT AN EXTENSIVE, SYSTEMATIC PROGRAM OF COLLECTING INFORMATION OF ECONOMIC VALUE--LARGELY FROM OPEN SOURCES--AND DISSEMINATING IT TO BUSINESS LEADERS.

IN THE FIFTH PATTERN, A GOVERNMENT COVERTLY TARGETS SENSITIVE WEAPONS TECHNOLOGY BY WORKING THROUGH FRONT ORGANIZATIONS, MILITARY ATTACHES, AND SPECIAL INTELLIGENCE UNITS THAT OPERATE OUTSIDE OF REGULAR INTELLIGENCE ORGANIZATIONS AND MAY BE DIRECTLY SUBORDINATED TO TOP NATIONAL LEADERS. A HIGH PREMIUM IS PLACED ON CLANDESTINITY IN THE PROCESS OF DIVERTING THE TECHNOLOGY AND ON DECEPTION IN PREVENTING ITS ACQUISITION FROM BECOMING KNOWN LATER.

AN EMERGING SIXTH PATTERN IS THAT OF INTELLIGENCE ENTREPRENEURS PREPARED TO SELL THEIR SERVICES EITHER TO FOREIGN GOVERNMENTS OR TO PRIVATE ORGANIZATIONS.

IT IS IMPORTANT FOR US TO MAKE THESE DISTINCTIONS ABOUT DIFFERENT PATTERNS OF ACTIVITIES. DOING SO HELPS IN ANALYZING AND UNDERSTANDING THE PROBLEM; IT ALSO HELPS IN DECIDING WHAT SORT OF RESPONSE IS APPROPRIATE IN PARTICULAR CASES. OBVIOUSLY, WE DO NOT HAVE THE SAME LEVEL OF COUNTERINTELLIGENCE INTEREST IN ALL TYPES OF FOREIGN COLLECTION ACTIVITY. FOR EXAMPLE, THE ACQUISITION OF UNCLASSIFIED INFORMATION, THROUGH OPEN CHANNELS, WITHOUT INVOLVEMENT OF A FOREIGN INTELLIGENCE ORGANIZATION, IS NOT A LEGITIMATE CONCERN OF US COUNTERINTELLIGENCE. AT THE SAME TIME, IT IS ESSENTIAL THAT WE MONITOR AND DEFEND OURSELVES AGAINST MORE SINISTER ACTIVITY.

WHAT WE DO WITH INFORMATION. LET ME NOW ADDRESS WHAT WE DO WITH THE

INFORMATION WE ACQUIRE ON FOREIGN ECONOMIC ESPIONAGE.

FIRST, WE PROVIDE INFORMATION ABOUT AND ANALYSIS OF FOREIGN ECONOMIC INTELLIGENCE COLLECTION TO POLICYMAKERS IN THE EXECUTIVE BRANCH AND TO THE HOUSE AND SENATE INTELLIGENCE COMMITTEES.

SECOND, WE PROVIDE DETAILED COUNTERINTELLIGENCE BRIEFINGS TO CONTRACTORS WORKING ON CLASSIFIED PROJECTS FOR CIA. WE ALSO PARTICIPATE IN BRIEFING PROGRAMS RUN BY OTHER GOVERNMENT AGENCIES FOR CONTRACTORS.

THIRD, IN COORDINATION WITH THE FBI WE INFORM AN INDIVIDUAL COMPANY IF WE DETECT AN INTELLIGENCE OPERATION DIRECTED SPECIFICALLY AGAINST IT OVERSEAS. IN ALL SUCH CASES, WE TAKE CARE TO PROTECT SOURCES AND METHODS. THIS SOMETIMES REQUIRES THAT THE INFORMATION BE PROVIDED IN A GENERIC FASHION, BUT WE USUALLY FIND A WAY TO TELL THE COMPANY WHAT IT NEEDS TO KNOW TO TAKE CORRECTIVE ACTION.

FOURTH, WE MAINTAIN CLOSE LIAISON WITH OTHER US GOVERNMENT AGENCIES. IF WE COME ACROSS INFORMATION THAT DOES NOT FALL WITHIN OUR PURVIEW, WE PASS IT TO THE APPROPRIATE DEPARTMENT. IF WE BECOME AWARE OF AN ACTIVITY THAT MAY BE A VIOLATION OF US LAW, OR DETECT AN INTELLIGENCE OPERATION DIRECTED AGAINST AN AMERICAN COMPANY, WE INFORM THE APPROPRIATE AGENCY. CONCERNING HOSTILE ACTIVITIES ABROAD, WE MAINTAIN CONTACT WITH THE STATE DEPARTMENT, SO THAT A DIPLOMATIC DEMARCHE CAN BE CONSIDERED. WE PASS TO THE COMMERCE DEPARTMENT INFORMATION ABOUT FOREIGN ECONOMIC DEVELOPMENTS.

COOPERATION WITH THE FBI. I WOULD LIKE TO SAY A LITTLE MORE ABOUT CIA'S COOPERATIVE RELATIONSHIP WITH THE FBI, WITH WHOM OUR COUNTERINTELLIGENCE PEOPLE ARE IN TOUCH ON A DAILY BASIS. CIA IN SEVERAL WAYS PROVIDES SUPPORT TO THE FBI AS IT CARRIES OUT ITS LAW ENFORCEMENT RESPONSIBILITIES IN COUNTERESPIONAGE. CIA PROVIDES THE FBI WITH LEADS WE

COLLECT OVERSEAS TO ILLEGAL ESPIONAGE ACTIVITIES AGAINST US INTERESTS. THE FBI CAN THEN INITIATE AN INVESTIGATION OF THE LEAD, WITH THE AGENCY CONTINUING TO BE INVOLVED IN THE OVERSEAS ASPECT TO SUPPORT THE FBI'S EFFORTS. CIA ALSO USES ITS RESOURCES TO TRACE INDIVIDUALS AND TO ASSIST THE FBI'S COUNTERINTELLIGENCE REQUIREMENTS WITH OUR ASSETS OVERSEAS.

CIA ALSO COOPERATES CLOSELY WITH THE FBI IN OUR INDUSTRIAL BRIEFING PROGRAM. FINALLY, CIA AND FBI COLLABORATE IN THE AREA OF COUNTERINTELLIGENCE ANALYSIS--BY EXCHANGING DATA, PARTICIPATING IN COMMUNITY ANALYTICAL CONFERENCES, AND PRODUCING JOINT ANALYTICAL ASSESSMENTS.

LOOKING AHEAD. LET ME SAY IN CLOSING THAT MONITORING AND ASSESSING THE FOREIGN INTELLIGENCE THREAT TO US ECONOMIC INTERESTS IS LIKELY TO ASSUME GREATER IMPORTANCE FOR THE US INTELLIGENCE COMMUNITY IN THE FUTURE. CONCEPTUALIZING THE ISSUES WILL CONTINUE TO BE COMPLEX, AS WE ATTEMPT TO DEFINE WHAT ACTIVITIES CONSTITUTE ESPIONAGE,

AND SEEK POLICY GUIDANCE ABOUT WHAT INTERESTS ARE "AMERICAN"--CONSIDERING THE MULTINATIONAL OWNERSHIP OF MANY CORPORATIONS, FOR EXAMPLE. WE WILL NEED TO SURMOUNT ANY CONSCIOUS OR SUBCONSCIOUS TENDENCY TO APPLY A DOUBLE STANDARD--WHICH COULD LEAD US TO DOWNPLAY HOSTILE ACTIVITIES IF CONDUCTED BY CERTAIN COUNTRIES. AT THE SAME TIME, WE WILL NEED TO AVOID THE PITFALL OF EXAGGERATING THE THREAT AS A MEANS OF JUSTIFYING BUREAUCRATIC BUDGETS, SATISFYING A LONGING FOR NEW "ENEMIES" TO REPLACE THE OLD, OR RATIONALIZING OUR NATIONAL ECONOMIC PROBLEMS.

Mr. BROOKS. Dr. Hearn.

**STATEMENT OF DR. JAMES J. HEARN, DEPUTY DIRECTOR,
INFORMATION SYSTEMS SECURITY, NATIONAL SECURITY
AGENCY**

Dr. HEARN. Thank you, Mr. Chairman. Thank you for the opportunity to speak on behalf of the National Security Agency.

I would like to begin by acknowledging, as you are certainly aware, that NSA's role in the protection of sensitive unclassified information is defined by the Computer Security Act of 1987. Other than for the protection of information, known as the Warner amendment information, NSA's role in this area is to act as a technical adviser to the National Institute of Standards and Technology, which I will refer to hereafter as NIST.

In this respect, I believe our research and development aimed at the protection of classified information has provided significant carryover into the unclassified sector, providing products and processes that can protect both government and private information.

The history of my organization and our view of the considerations involved in the protection of information is contained in my written testimony. What I would like to do in the next few minutes is to highlight some examples of current activities that I believe safeguard vital U.S. information.

The Computer Security Act of 1987, and other efforts of the Congress and the executive branch, have significantly increased awareness in the Federal Government of the computer security problem. As we heard from the DCI and from Judge Sessions, the intelligence and counterintelligence communities are engaged in detailing the foreign threat to U.S. communications systems. The Computer Security Act called for increased planning and training in the Federal Government. The plans were made, critiqued, and are being implemented.

NSA and NIST have a major effort under way jointly in the computer security arena to produce a Federal computer security criteria which should provide a basis for computer security throughout the Government. U.S. industry strongly supports this joint activity.

One successful application of current technology from the classified arena is a product called the Secure Telephone Unit, Generation III. This program has increased the number of secure telephones from fewer than 10,000 6 years ago to over 200,000 at the current time. This instrument is on U.S. Government desks all around the world and its use has become part of the normal business routine, especially in the national security community. It proved vital to providing tactical secure voicecoms in Desert Storm. In addition to its voice use, each Secure Telephone Unit has a data capability providing convenient and well-connected data and fax security.

Cooperation between NSA, NIST, and the Secure Telephone Unit manufacturers has extended this success program into the unclassified arena. The original Secure Telephone Unit was designed for the national security community, with the ability to interoperate with Secure Telephone Units designed for the unclassified user. Use of NSA-invented and industry-implemented security tech-

nology in each phone means the classified community can now securely interoperate with parts of the Government that handle sensitive unclassified information.

One application of this telephone unit architecture is relevant to the subject of this hearing. The Overseas Security Advisory Council involves the State Department sharing sensitive security information with U.S. companies operating overseas. NSA, NIST, and State, working in concert, have begun using versions of Secure Telephone Unit products to secure communications between U.S. Embassies and overseas sites of these companies.

Almost all of the recent penetrations of unclassified computer systems studied by several organizations, including the GAO, were shown to result from bad security practices such as poor password management, or failure to correct known operating system flaws or physical security weaknesses. The penetrations were the result of adversaries taking advantage of the easy vulnerabilities. Encryption technology is only part of the solution. Better awareness, training, planning, and technology will help our security posture, but the key is providing motivation.

An example of the positive effects of awareness and motivation was contained in the recent Michelangelo virus activity of March 6 of this year. Original estimates were that as many as 15 to 18 percent of U.S. personal computers could lose data due to that virus. However, the publicity attendant to this event led to a heightened awareness which caused fear over the loss of data. Existing techniques were used on an unprecedented scale and resulted in little damage to systems around the country. Why? Because people appreciated the value of the information they stood to lose and were willing to go out of their way to protect it.

If it were possible to treat our information with the same care as we did this first week in March, the United States would take a significant step in information security.

In summary, we need to focus on the information to be protected and its value, in addition to the mechanisms of protection. Second, tools exist today to significantly improve the U.S. Information System Security posture.

Thank you for the opportunity to present these views. I would be glad to try to answer any questions you may have.

Mr. BROOKS. Thank you, Doctor.

[The prepared statement of Dr. Hearn follows:]

**PREPARED STATEMENT OF DR. JAMES J. HEARN, DEPUTY DIRECTOR,
INFORMATION SYSTEMS SECURITY, NATIONAL SECURITY AGENCY**

Mr. Chairman:

Thank you for the opportunity to speak today and discuss the protection of sensitive U.S. economic information from the foreign collection threat.

First let me acknowledge, as you are certainly aware, that NSA's role in the protection of sensitive unclassified information is limited by the Computer Security Act of 1987. Other than for the protection of information specified in Title 10 USC 2315 or Title 44 USC 3502 (2), known as Warner Amendment information, NSA acts as technical advisor to the National Institute of Science and Technology (NIST). Our research and development, aimed at the protection of classified information, has provided significant carry-over into the unclassified sector, providing protection for both government and private information.

What I hope to leave you with today are two thoughts:

- People need to focus on the value of the information they hold, and its need for protection, and,
- Tools exist today to significantly improve the U.S. Information System Security (INFOSEC) posture.

I represent the Informations Systems Security Organization within the National Security Agency. My organization is responsible for developing policies, technology, and systems that protect classified information. Since our inception in 1952 we have performed over 200,000 man-years of research on the development of information systems security. Both directly and through our collaboration with NIST we have transferred much of this technology to the unclassified world. Our operation of the National Computer Security Center has given us the means to work directly with vendors in the development of Computer

Security technology which is being used to protect classified and unclassified information both inside and outside the government.

The driving force behind our efforts, NIST's efforts, and the efforts of this committee is, that information has value; in fact, information is equity, and there must be a focus on protecting that asset. Classified-versus-unclassified is just a formal question of relative value. Identifying the threat, (foreign or domestic), is secondary. By focusing on the fact that information has value and needs to be protected, many extraneous concerns are eliminated.

This may seem obvious, but our 40 years in the INFOSEC business has taught us that security will always be subordinate to operations:

- When most organizations look to the future, security is underplanned and underfunded, in favor of maximizing operational capability.

- And, in day-to-day operations, security is often ignored, in the name of operational necessity, or even convenience.

The need to protect the information is forgotten in the press of day-to-day activity.

Our relatively new name, Information Systems Security, highlights some of the conclusions we have reached after carefully examining where we need to head in the future based on what we see developing around us.

This same thinking forms the thrust of my remarks today --

- How can we assure that information vital to the interests of the U.S. remains in the proper hands; what have we been doing right; and, what do we need to do better? To understand where

we are going, let me talk about how we got here.

At NSA our early years of protecting information were devoted to communications security, and we were known as the COMSEC organization. We focused on the protection of radio, telephone, satellite and other telecommunications technologies developed to help government agencies and military departments accomplish their missions. Each new communications development was met with a new COMSEC system. In almost every case our equipment was an add-on to the system.

This meant that if you were a soldier who carried a radio, if you were to secure your communications against eavesdropping, you carried an extra piece of gear, a COMSEC "black box." There was some honest resistance to carrying the extra load, but usually the COMSEC was dutifully carried and cautiously protected, because the soldier was motivated to do so. His life might well depend on his ability to call for help or communicate his unit's intentions without giving information to an enemy listener.

The COMSEC equipment made communication more difficult, added weight, and needed special protection, but it was used because the soldier understood its value in terms of personal security.

The value of military information in a war scenario is easy to understand. However, in peace, it is not so obvious. During normal operation and exercises we found that the COMSEC remained in the vault and wasn't used. We undertook a concerted effort to inform all holders of classified information of the peacetime threat to that information. We also significantly changed the rules for controlling COMSEC equipment, declassifying most of it in 1984. Peacetime use

of COMSEC has increased, but only with constant effort.

We have found that computer security is more difficult to motivate. In wartime, the physical risks to computer systems are understood, but risks to information are less well-defined. In peacetime, computer security measures, which always exact costs in performance and convenience, are not tolerated by many users, especially those outside the military and intelligence cultures.

Keep in mind that computer operations evolved from a culture of the 1960's where computer centers were viewed as no different from other locations processing or storing sensitive data. They were protected the same as any other office or warehouse, with fences, guards, and controlled access based on security clearances. The computer operated in a tightly controlled area and people who used it did so by passing in decks of punched cards and later receiving printed output in return. This approach not only physically protected the computer, it protected its information as well. Only those with proper clearances got access to the data and the human interface enforced the security policy. Physically limited access significantly reduced the likelihood of compromise.

Computers which shared data did so with a physical exchange of media, usually tape, and users had to wait hours between putting data in and getting results out.

By the late 1970's the world's basic data processing architecture had changed. Systems became networked, allowing distributed processing. Remote terminals led to direct electronic access into the once-isolated computer systems. As a result we worked on security solutions for the computer systems, trust technology, and COMPUSEC was born.

As personal computers became more powerful and ubiquitous, the capabilities available on everyone's desktop and their ability to interact with the information processing system increased significantly. The distinction between computer and communications became blurred. This, in turn, caused a blurring of COMSEC and Computer Security and showed us by 1990 that separating the two disciplines didn't make sense anymore. We found that we were making an artificial distinction between computers and communications which did allow us to attack the problem in fragments. However, the fragmentary solutions, when put together in a real system, left gaps in protection, which meant the information was still vulnerable.

Solving this meant focusing on the entire system. The hardware, the software, the communications, the people, the facilities, the procedures must all be evaluated together. The technology could not be evaluated alone, and so we became the Information Systems Security Organization.

As documented here today and in many other instances, the information in U.S. Government computer and communications systems and in U.S. private sector systems is vulnerable. It is certainly possible for an adversary to gain access to the information in many of our systems. Moreover, as also noted here today, our foreign adversaries are taking advantage of our vulnerabilities. This foreign threat, combined with our domestic vulnerabilities, leads to grave concern.

So, what do we do? Many positive steps are underway.

- The Computer Security Act of 1987 and other efforts of the Congress and the executive and the private sector have significantly increased awareness of the Computer Security problem.

- NSA and others have been detailing the foreign threat to U.S. communications systems for years.
- The Computer Security Act called for increased planning and training. The plans were made, critiqued, and are being implemented.
- The Act calls for the establishment of standards. Some of these, such as the Digital Signature Standard, are beginning to emerge. Others are being actively pursued.
- NSA and NIST have a major joint effort underway in the Computer Security arena to produce a Federal COMPUSEC Criteria which will expand the scope of our current DoD trusted product program and provide a basis for Computer security throughout the government.
- The largest current technological challenge we face is the development of multi-level secure systems. Through 1999 my organization plans to spend several hundred million dollars on technology to enable the development of these systems. This work will have direct applicability to the protection of unclassified sensitive information.

One successful application of current technology in the classified arena is the STU-III. This program has increased the number of secure telephones from fewer than 10,000 to over 200,000 in the past five years. This instrument is on government desks all around the world and its use has become a part of the normal business routine. It proved vital to providing tactical security in Desert Storm. In addition to its obvious voice use, each STU-III has a data capability, providing convenient and well-connected data and fax security.

Cooperation between NSA, NIST and the STU-III manufacturers has extended this successful program into the unclassified area. The original STU-III was designed with the ability to interoperate with a STU-III designed for the unclassified user. Use of NSA-invented, industry-implemented COMSEC techniques in each phone means the classified community can now securely interoperate with parts of the government that handle sensitive unclassified information, and they, in turn can use the same phone to secure their communications with the private sector.

One application of this architecture is relevant to the subject of this hearing. The OSAC (Overseas Security Advisory Council) involves the State Department sharing sensitive security information with U.S. companies operating overseas. NSA, NIST, and State, working in concert, have begun using versions of the STU-III equipment to secure communications between U.S. embassies and overseas sites of these companies.

Properly used, these devices can secure voice, data and fax transmissions, but they must be used, and, when in use, can only protect information for the few seconds it is being transmitted from place to place. This may be when the information is most vulnerable, but the STU-III cannot ensure that information is not available to an adversary at some other time in its life.

These are examples of on-going work to improve the protection of sensitive U.S. information and that significant effort is underway to solve the remaining technical impediments to system security. However, the attraction of new technologies and new applications, some aimed at new threats and some at improving the "user-friendliness" of INFOSEC products, should not obscure the large body of

INFOSEC tools already available.

All the recent penetrations of unclassified systems studied by NSA, NIST, and GAO were shown to result from bad security practices such as poor password management, or failure to correct known operating system flaws or physical security weaknesses. The penetrations were the result of adversaries taking advantage of "low-hanging fruit" and more technology would not have helped in those cases. We would make a significant step forward if we could force an adversary into the more sophisticated attacks needed to penetrate existing COMPUSEC protection. Now, however, existing fixes to the COMSEC and COMPUSEC problems are not being used. We could make our adversaries' lives much tougher, just by fully employing what is now available.

More awareness, training, planning, money, people, and technology will help our security posture, but the key is providing motivation. Security will never be free, whether in terms of dollars, convenience, or performance, and to justify security we need to return to the critical thought--The information is important.

If you recall the COMSEC example I cited earlier, where the desire to stay alive outweighed the bulk and inconvenience of the COMSEC box, you can see the point. Proper application of existing tools can go a long way toward improving our Information Security posture.

An example of this is the recent Michaelangelo virus activity. Original estimates were that as many as 15-18% of U.S. personal computers could lose data due to that virus. However, publicity led to heightened awareness which caused fear over the loss of data. Existing techniques were used on

unprecedented scale and resulted in little damage to systems around the country. Why? Because people appreciated the value of the information they stood to lose, and were willing to go out of their way to protect it.

If it were possible to treat our information with the same care as we did the first week in March, the U.S. would take a significant leap in information security.

In summary,

- We need to focus on the information to be protected, and its value, not on the mechanisms of protection.

and,

- Tools exist today to significantly improve the U.S. Information System Security (INFOSEC) posture.

We need to convince people that in the 1990's, equity is not measured just in terms of cash, buildings and inventory, but also in terms of information. If people understand and appreciate the value of the information they hold, and the value of keeping it from their foreign competitors, we will take a major step to reducing the vulnerabilities of our information systems.

Thank you for the opportunity to present these views.

I'd be glad to answer any questions you may have.

Mr. BROOKS. According to a December 21, 1991, New York Times article, a presidentially directed study of intelligence activities was to be completed and recommendations made for structural changes, budget, and possible new legislation by March 20, 1992. We're in the process, I might say, of requesting a copy of that directive.

Did these recommendations, gentlemen, include any significant changes to the intelligence and counterintelligence authorities of the FBI, the CIA, or NSA?

Mr. GATES. Mr. Chairman, let me take a crack at that.

Mr. BROOKS. Director Gates.

Mr. GATES. Yes, it did. The intelligence community has been engaged in collection on economic intelligence issues for some years. But this national security directive really expanded and made more specific policymaker direction and priorities in terms of what the policy community, up to and including the President, wants us to collect against.

About 40 percent of the requirements that were approved by the President are economic, either in part or in whole. They deal with questions in the whole arena of information needed to level the playing field, what foreign governments are doing to disadvantage the United States and not play by the rules, not abide by agreements and so forth, questions about predatory and subversive foreign targeting of U.S. industry, as well as these questions we've been discussing today about foreign counterintelligence. So for the first time, I think this national security directive codifies and prioritizes the economic requirements being placed on the intelligence community.

Mr. BROOKS. Did you have any comment on that, Judge?

Mr. SESSIONS. Mr. Chairman, with the FBI, of course, we operate in the counterintelligence arena and we will await being informed about the nature of the information that was gleaned from the study. I'm confident it will be shared with the FBI in due course.

Mr. BROOKS. Dr. Hearn, any comment on that?

Dr. HEARN. I have nothing further to add.

Mr. BROOKS. All right.

Director Gates, in your testimony you indicated the CIA will be focusing on efforts of foreign intelligence services to influence government decisionmaking by lobbying and other means. What specifically is the threat here and how does the CIA plan to address this problem?

Mr. GATES. I think, Mr. Chairman, that the basic nature of the problem is the degree to which activities that are undertaken in this country by foreign businesses are being driven by foreign governments. Our objective is to provide information to our policymakers on the activities of foreign businesses in collusion with foreign governments. It's the governmental role, the intelligence services, or actually any part of a foreign government, acting in concert with their business to disadvantage the United States, that is of interest to us. So our collection activities would be aimed at determining the role of foreign governments in these lobbying activities and making that known to the policy community in the executive branch and to the Congress.

Mr. BROOKS. Now, you know that the Toshiba Corp., when Congress attempted to legislate sanctions against them for selling sen-

sitive DOD technology to the Soviets, the lobbying by Toshiba was the best that money could buy. Even the DOD complaints were sort of quieted. But I trust that this is an area within the United States that would be the jurisdiction of the FBI, since it's occurring here in this country, right in this city as we speak, and I hope that this area does not drift off into your area, Dr. Hearn, or you area, Director Gates.

You understand what we're talking about.

Mr. GATES. Yes, sir. I will defer to Judge Sessions. We would be involved only to the extent that the Japanese Government and information that we collect appropriately overseas would be involved in that.

Mr. BROOKS. But, you see, that comes right back into the FBI's jurisdiction and responsibility.

Mr. GATES. Yes.

Mr. BROOKS. I don't want this new effort to change those lines of authority too much. You are at least cooperating very well together now, which is a new change—really, this happens. Government agencies are just as persnickety as individuals are, you know, and sometimes they don't get along with each other too well. They're suspicious of each other, just like they're foreign governments. That's one of the major problems that the executive has, getting all the agencies to work together—any executive, Bush or Carter or Johnson or—well, Reagan didn't worry much about how it worked.

[Laughter.]

Mr. BROOKS. But Ford did and Eisenhower did. They had the agencies and wanted them to work together. Now you all are doing that much better. Surely it would be more helpful.

Did you have a comment on that, Judge?

Mr. SESSIONS. No, Mr. Chairman.

[Laughter.]

Mr. SESSIONS. Except to say that I adopt the chairman's observation that the relationships between the CIA and the FBI are excellent. And the working relationship isn't just superficial. It goes all the way down into the workings with which the FBI is charged and the CIA is charged in the counterintelligence area.

I chair the Advisory Group on Counterintelligence and the work that has been produced there, both through the group itself and its counterintelligence board, and its response to DCI, I think will reflect that we have stayed right on top of our counterintelligence responsibility, not only in the counterintelligence area but in the criminal area as well.

Mr. GATES. Mr. Chairman, could I add just one point?

Mr. BROOKS. Yes, sir.

Mr. GATES. I just wanted to add—and to get at the first part of your question—that we do not see, as a part of this effort involving economic intelligence or counterintelligence, any change in the lines of responsibility or authority between the intelligence community or the FBI. In fact, we will not be seeking any new authorities from the Congress or the executive in terms of the role that we play.

Mr. BROOKS. Would you please give us a summary of the CIA-sponsored study entitled "Japan 2000," which examined Japanese

international trading practices? Could you give us a comment on that?

Mr. GATES. The only thing I could say, Mr. Chairman, is that that study took place while I was still working at the White House and I'm not familiar with the details of it. I would like to be able to provide that for the record, if I might.

Mr. BROOKS. Without objection.

[The information follows:]

Central Intelligence Agency

MAY 28 1992

Washington, D.C. 20505

22 May 1992

The Honorable Jack Brooks
Chairman
Subcommittee on Economic and
Commercial Law
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

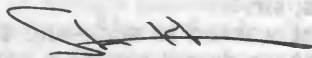
Dear Mr. Chairman:

The Director has asked that I provide you with a summary of the "Japan 2000" report as requested in your 29 April hearing.

In addition to providing a summary, we want you to understand the background of this report. On the Agency's behalf, the Rochester Institute of Technology conducted a seminar regarding the future of Japan. After the seminar, an employee of RIT prepared an unclassified document entitled "Japan 2000." The report is not a CIA document and, as its author stated in the foreword, "The views expressed in the report do not constitute the policy or opinion of RIT, the RIT Research Corporation, RIT's officers, trustees, faculty, staff, or students."

The attached statement from the introduction to the draft report provides a brief summary of the document.

Sincerely,



Stanley M. Moskowitz
Director of Congressional Affairs

Enclosure

Part One examines the social, technological, and political changes that have resulted in the present global marketplace and the shift to a transnational economy. The nature and role of power are fundamental to the success of this shift. The Japanese perception and use of power is profoundly important because the Japanese Paradigm applies power differently than the West.

Part Two raises the question of the possibility of Japanese Paradigm eclipse and examines the global impact of such an event. In light of a world turned upside down, observations are made concerning the concept and context of US national security in an atmosphere that is fragmented and undergoing a power shift in all secrets and strata, worldwide.

The conclusions, designed to provide a proactive, conceptual framework for future policy, strategy, and action-oriented decision making include observations and matters requiring attention based on information contained in the first two chapters.

In addition to biographical information about the discussants, a glossary of Japanese terms, and references are two appendices: an abbreviated economic, demographic, political, and sociological sketch of Japan and the Imperial Oath of 1968.

JAPAN 2000

A Study of the Japanese Future

Edited by J. R. H. Brown and J. R. H. Brown
1991

Mr. BROOKS. I would say that in part 2 it pointed out that Japan controls probably the most effective and efficient lobbying/influence peddling machine in the United States, surpassing all special interest groups, unions, industries, and both political parties. It is focused, relentless, amply funded, and frighteningly successful. It goes on and says that political exploitation is pervasive, even institutionalized. The Japanese lobby equally supports both major political parties in Congress—not me, I might add and I'm not angling for it, either, I guarantee you—and spends an estimated \$400 million a year on political campaigns designed to capture markets in targeted technologies and industries by influencing trade policies.

In addition, it is estimated that the Japanese spend over \$300 million yearly influencing grassroots public opinion on various issues. That's more money than Perot is going to spend.

[Laughter.]

Mr. BROOKS. Without objection, we will put this in the record, and we will accept your comments for the record, sir.

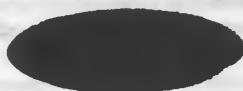
[The document follows:]



JAPAN 2000

Unedited Prepublication Copy

Please Destroy All Previous Editions
5/1/91



Japan has also achieved greater equality than almost any country in the West. Most important, the secret of Japan's success relates, at least in part, to the non-western organizational principles. Furthermore, the same phenomenon is occurring in Hong Kong, Singapore, South Korea, and Taiwan; what we seem to be witnessing is not simply a Japanese challenge but an Asian challenge, a development that cannot but call into question the very basis of the pax-Americana.

Exploiting Western Systems

Political Exploitation

Japan controls probably the most effective and efficient lobbying/influence-peddling machine in the U.S., surpassing all special-interest groups, unions, industries, and both political parties. It is focused, relentless, amply funded, and frighteningly successful.

A recent battle pitted Japan against General Motors, Chrysler, Ford, and the United Auto Workers. Japanese pick-up trucks were classified as "automobiles" to permit importation under a lower automobile duty schedule. Obviously, this action would hurt U.S. auto makers and their unions, yet, remarkably, Japan's lobbyists won. In addition to hiring a former presidential aide as a lobbyist, Suzuki Motor Company engaged America's best public relations firms in New York and Washington to launch a major public relations/lobbying campaign stating that refusal of the waiver would "raise the cost to consumers" and "harm U.S./Japanese relations." When the message was picked up and echoed by Congress, the executive branch capitulated. This public relations coup was accomplished at a cost estimated by Pat Choate at \$3-4 million and resulted in evasion of over \$500 million annually in import duties. No concessions whatsoever were made to any U.S. demand. Even by Japanese standards, \$500 million is a terrific return for a \$4 million investment—12,500 percent! A greater affront to our nation, however, was that this incident confirmed the vulnerability and gullibility of some Washington policy makers.

In 1982, Japan's National Institute for Research Advancement conducted a major study of the backgrounds, functions, and career patterns of the nearly 30,000 people who fill critical policy-making positions in the U.S. government. The results were published in 1984: "The Role of the Congressional Staff in the U.S. Decision Making Process" is phenomenal both for the insight it provides for Japan and the use to which it was put.

Based on this document, a meticulously planned and executed offensive was undertaken on Capital Hill, involving elaborate hospitality as well as all-expense-paid "fact finding" trips to Tokyo. Governors, U.S. trade representatives, former Government officials, including past members of the executive branch, legislative aides, and others, were and are targets. Through this study and others, which are ongoing, the Japanese possess probably the best data base on U.S. federal officials and other targeted government areas of influence than any intelligence service in the world.

Political exploitation is pervasive, even institutionalized. The Japanese lobby equally supports both major political parties in Congress and spends an estimated \$400 million a year on political campaigns designed to capture markets in targeted technologies and industries by influencing trade policies. In addition, it is estimated that the Japanese spend over \$300 million yearly influencing grassroots public opinion on various issues. Their political counsel is nearly faultless. They rarely make mistakes, and when they do, they correct them immediately. Witness the recent Yosemite National Park concession controversy, resulting from Japanese purchase of the company owning the concession to this almost sacred national monument. When it appeared that the controversy would damage Japan's image in the U.S., the affair was rapidly defused and disappeared from the political and public view—there were larger fish to fry.

Intelligence/Propaganda Exploitation

Japan's elaborate system for political and economic intelligence is conducted through the various trading companies down to the office level. Using what has been referred to as the "vacuum cleaner" approach, Japanese trading companies are provided with information by numerous sources, including the internationally represent***.

Mr. BROOKS. At the conclusion of your comments, without objection, I would, by unanimous consent, like to include a letter from Congressman Frank Horton, the ranking member of the Government Operations Committee, who has some very perceptive comments on this very subject. At this point we will put that in the record.

[The letter follows:]

JOHN COVATTA, JR., MICHIGAN
CHAIRMAN
CARLOS COLLINS, ILLINOIS
ELIOT ENGEL, DELAWARE
HENRY A. WAXMAN, CALIFORNIA
TED WEISS, NEW YORK
KIMBLE EYAL, DELAWARE
STEPHEN L. HEAL, NORTH CAROLINA
BOUR BARRIAS, JR., GEORGIA
TOM LANTOS, CALIFORNIA
ROBERT E. VOISE, JR., WEST VIRGINIA
BARBARA BOHRER, CALIFORNIA
MAJOR R. DOWNEY, NEW YORK
BONAPARTE TOWNS, NEW YORK
SEN BERNARD ALABAMA
GERALD R. RUCICIA, WISCONSIN
ALBERT B. BURSTAMANTE, TEXAS
MATTHEW D. MARTINEZ, CALIFORNIA
DONALD H. PAYNE, NEW JERSEY
GARY A. COHEN, CALIFORNIA
PATRY T. SMITH, MAINE
RAY THORNTON, ARIZONA
COLLIN C. PETERSON, MINNESOTA
ROSA L. BLAUM, CONNECTICUT
CHARLES J. LINDER, OHIO
JOHN W. COLE, JR., ILLINOIS

ONE HUNDRED SECOND CONGRESS

Congress of the United States House of Representatives

COMMITTEE ON GOVERNMENT OPERATIONS

2167 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

FRANK HORTON, NEW YORK
BAKERS VINDICITY MEMBERS
WILLIAM F. CLINGER, JR., PENNSYLVANIA
AL SECANDALESS, CALIFORNIA
J. DENNIS HARTNETT, ILLINOIS
JOHN L. EYAL, ARIZONA
CHRISTOPHER SHAYNE, CONNECTICUT
STEVEN SCHIFF, NEW MEXICO
C. CHRISTOPHER COLE, CALIFORNIA
ORLAND THOMAS, WYOMING
KELARA ROE-LEWIS, FLORIDA
RONALD R. BUCHHEIT, RHODE ISLAND
BICK DANNIS, NEW JERSEY
WILLIAM R. BULLY, JR., NEW HAMPSHIRE
DAVID L. HOBSON, OHIO
SCOTT L. ELUS, WISCONSIN

EDWARD LAMERS, VERMONT
REDFORDSIST

MAJORITY-(205) 225-2061
MINORITY-(205) 225-0076

April 28, 1992

RECEIVED

APR 28 1992

JUDICIARY COMMITTEE

The Honorable Jack Brooks
Chairman
Committee on the Judiciary
2138 Rayburn HOB
Washington, D.C. 20515

Dear Jack:

I had planned to testify before your hearings today on economic espionage, but some scheduling problems just do not allow it. For the record, though, I would ask that you consider a few points on a subject that you and I have worked together on for as many years as you were Chairman of the Committee on Government Operations. That subject is the unfair trade practices of Japan and how Japan's actions, including economic espionage, affect and undermine the ability of the United States to retain high-paying manufacturing jobs, retain a critical manufacturing base, compete fairly in the international market, and more comprehensively, ensure a continued opportunity for American business and workers to compete head-to-head, and by the same rules, as every other major economic power.

As Americans, we do not have that opportunity today. Japan in particular has attacked with the skill of a surgeon's knife broad sectors of American industry. Its strategies include the dumping of products here at prices below the cost to manufacture them, a particular practice that has brought American consumer electronics, semiconductor and steel industries to their knees. At the same time, trade barriers are put in place in Japan that block the entrance to Japan's market of these and other products. Higher prices are charged in Japan for the same products being dumped abroad so that the dumping practices are subsidized.

These and other trade practices of Japan are put in place through an industrial organizational structure, the embodiment of which is the "keiretsu." Under this structure, competition is limited and controlled, and the trade, production and sales policies of entire industries are directed with little if any regard for antitrust concerns held by the United States and most industrial nations.

Page Two

Indeed, Japan's approach to dominating world markets is effective. It needs to be understood. Studies illuminating Japanese economic practices should be encouraged and analyzed. Mr. Andrew Dougherty, a constituent of mine, oversaw a study of Japan's economic strategies during his tenure as Executive Assistant to the President of the Rochester Institute of Technology. The study, titled Japan 2000, attracted scholars, business and government leaders from around the world. The study was funded largely by the CIA.

Japan 2000, however, became embroiled in controversy. Its message apparently was too strong. While some in American industry embraced the study's message as gospel, others, particularly those in or professionally involved with our government, felt that it might create diplomatic problems because of its conclusion, which was of no great surprise to me, that Japan seeks to economically dominate world markets.

Of course, some Japanese government and industry officials were outraged and some of those involved with the report's construction moved to distance themselves from its final content. Apologies were made to Japanese officials for whatever reason. To my knowledge, though, no delegation from Japan has visited the United States apologizing for one of the best-selling books in Japan "The Japan That Can Say No." And Japanese government officials who criticized the American worker are in no danger of losing their elected positions.

Instead, American government officials continue their meetings with Japanese government officials over proposals to encourage Japan to remove its many tariff and non-tariff barriers. Today those talks take the form of the Strategic Impediments Initiative. The talks plod along. Progress plods along. But in no way does progress on these talks keep pace with the problems posed by increasing trade deficits. Nearly 30 years ago we recorded our first trade deficit with Japan - about \$235 million. We initiated talks with Japan at that time. Several hundred billion dollars in accumulated trade deficits later, growing at a rate of between \$40 billion and \$60 billion each year, those talks continue.

The bottom line to all of these talks can be reduced to simple and comprehensible terms. We are still not selling rice to Japan on any appreciable scale even though we produce at a fraction of what it costs to produce in Japan. Or citrus. Or vegetables. And a presidential mission returns from Japan with a promise, probably achieved after several grueling hours of difficult negotiations, to set a target for the purchase by the Japanese of 20,000 minivans, a promise that resulted in protests in Tokyo streets. Meanwhile, the two million plus Japanese cars purchased by Americans each year continues along. The Japanese economy continues along at full

Page Three

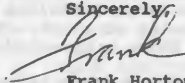
employment. And General Motors is laying off another 75,000 of its workers.

So, Mr. Chairman, I guess my point is this. I applaud you for holding this hearing. I hope it produces something worthwhile, and I am confident that it will. I hope, too, that you will ask the tough questions to the government witnesses you have testifying today, about their understanding of the difficulties our trade problems with Japan in particular, but any country really, whose practices prevent - to use your words - "full and open" competition. I hope you ask them about the importance of critical studies that illuminate these unfair practices, about their use of this information in changing our own trade practices and policies where they are not met with reciprocal trade environments. Their understanding, indeed their actions, on this subject is and are important. They are important because they ultimately will affect the families of those 75,000 workers who are losing their jobs, and of so many hundreds of thousands of others who face, have faced and will face the same situation because these unfair trade practices are tolerated.

Mr. Chairman, I also am encouraged by reports I hear that you are considering hearings and possibly legislation on the application of U.S. antitrust laws to foreign companies operating in the United States. Press reports indicate that the Justice Department, too, may have an interest in this area. Such a review, I believe is in the public interest. Such a review may create some discomfort for our allies in Japan and possibly other countries as well. Of course, Mr. Chairman, I have worked with you for a number of years. I am sure that criticism from abroad of actions you may take in the public interest will receive their due consideration. If I can be helpful in these areas, please let me know. In the meantime, I hope my comments in this letter have been useful.

With kindest personal regards,

Sincerely,



Frank Horton
Ranking Minority Member

Mr. BROOKS. Now, do you believe that U.S. industry should have the right to the best commercial cryptographic technology available to ensure privacy of sensitive business communications?

Mr. SESSIONS. Mr. Chairman, I can say, unequivocally, yes. It is absolutely essential that we not be in any way hampered in the technological advances that are bursting all around us. The only thing the FBI has insisted upon—and I listened to the earlier remarks, the testimony of the GAO—the only thing we insist upon is what was given to us by statute back in 1968; that is, to have the access which is court monitored, court sponsored, which is court reviewed, and further with our oversight committees in the Congress, and the Department of Justice, and every single possible oversight is given to that. But the technology must allow us access, and it must allow us to stay even with what we now have, or else we are denied the ability to carry out the responsibility which the Congress of the United States has given us.

Mr. BROOKS. Dr. Hearn, any comment on that?

Dr. HEARN. No, I have nothing further.

Mr. BROOKS. Director Gates.

Mr. GATES. No.

Mr. BROOKS. The GAO testified that it encountered some serious access problems with both the FBI and CIA while conducting its investigation of foreign economic espionage activities against U.S. corporations.

Would you give us an idea of why the problems occurred briefly and just what the legal basis was for some reluctance certainly to cooperate with GAO on this matter? And before you get carried away with that, Judge, you know, Congress never stated that the jurisdiction of the Intelligence Committee is exclusive. The House Intelligence Committee has indicated that it does not agree with the CIA on your position, Director Gates, or your predecessor's position, and has pointed out that House rule XLVIII stated "Nothing in this rule shall be construed as prohibiting or otherwise restricting the authority of any other committee to study and review any intelligence or intelligence-related activity, to the extent that such activity directly affects a matter otherwise within the jurisdiction of such committee."

My interest has been that the GAO be given access to executive branch records. You should cooperate with them as you do with each other, and with NSA and DOD, et cetera. Yes, Judge.

Mr. SESSIONS. Mr. Chairman, I will try to follow your admonition given here today. We have at the present time over 30 audits that are being conducted by the GAO within the FBI. There is a GAO office at the FBI that existed, had the label on the door, at the time I became Director—and it is there to this good day. We do have, of course, continuing criminal investigations, and we do not intend in those areas to shirk our responsibilities to protect our sources, our methods, our techniques, nor do we intend to allow the identities of our informants to be beyond our control. Therefore, when we do have these requests, it is within that context that we seek to work.

But I could not count our agency as being anything other than what I construe to be careful and cooperative, and we have worked with Chairman Edwards in connection with specific files over a pe-

riod of months to be sure that they do have the access. I don't mean to be defensive. I do intend to be cooperative within the framework of our capability.

Even in the classified area, we have not denied access on account of classification. We have simply tried to be sure that we carry out our responsibility as an investigative agency, charged with the responsibility of investigating those criminal activities so that we can pursue them and pursue them effectively.

Mr. BROOKS. Director Gates. You understand where we're coming from, you understand our position?

Mr. GATES. I do.

Mr. BROOKS. I think you need to continue that openness policy just a little bit more. I mean, open the door not just this much, but go on and open it. Just open that door. "Ouvrez la porte," as they say. That's in southwest Louisiana and southeast Texas where they say that.

Mr. GATES. They say that in Kansas, Mr. Chairman.

Mr. GLICKMAN. Mr. Chairman, he didn't just make that statement gratuitously about me. He is from my hometown, the Director of the CIA. I wanted you to know that. It's a very wonderful place to be from.

Mr. GATES. Mr. Chairman, I divide our approach to GAO into two parts. The first is, I believe that we can be cooperative with GAO on substantive matters such as the one that we are discussing here and able to provide them with information, including on a classified basis.

The only concern that over the years—the only place that a line has been drawn is in terms of the oversight role of the GAO itself in terms of intelligence operations and investigations into intelligence activities. Here, the Congress itself has established the Intelligence Oversight Committees in the House and the Senate to carry out this responsibility, a responsibility that was augmented some years ago by the addition to both staffs of an audit capability that would allow them to go into our books in a detailed and professional manner.

So we are certainly prepared, and, quite frankly, I think we at the outset—when the committee began to look at this foreign economic intelligence activity, I think that at first blush the intelligence community could have and should have been more cooperative with both the committee and the GAO, and that is one of the reasons why I came down here today.

But I think our position of long standing in terms of actual oversight of intelligence activities remains consistent with the intent of the Congress itself.

Mr. BROOKS. I would ask unanimous consent to put a letter in that we sent to Mr. Webster and a letter we received back from Mr. Webster on this subject.

[The letters follow:]

MAJORITY MEMBERS

JACK BROOKS, TEXAS, CHAIRMAN
 DON EDWARDS, CALIFORNIA
 JOHN COYNE, JR., MICHIGAN
 ROBERT L. MADDOL, KENTUCKY
 WILLIAM J. HUBER, NEW JERSEY
 MIKE STAN, OREGON
 PATRICIA SCHROEDER, COLORADO
 DAN GUCKERMAN, KANSAS
 BARNEY FRANK, MASSACHUSETTS
 CHARLES E. SCHUMER, NEW YORK
 EDWARD E. FUSHEE, OHIO
 HOWARD L. BERNAL, CALIFORNIA
 RICK BOUCHER, VIRGINIA
 HARLEY O. STADGERS, JR., WEST VIRGINIA
 JOHN EVYATT, TEXAS
 MIKE LEVINE, CALIFORNIA
 GEORGE E. BANGHEIMER, ILLINOIS
 CHAS. A. WASHINGTON, TEXAS
 PETER HOAGLAND, NEBRASKA
 MICHAEL J. SPIRTES, OREGON
 JOHN F. REED, RHODE ISLAND

ONE HUNDRED SECOND CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-9210

MINORITY MEMBERS

HAMILTON FIRM, JR., NEW YORK
 CARLOS J. MOOREHEAD, CALIFORNIA
 HENRY J. WIDE, ILLINOIS
 P. JAMES BREWSTER, JR., WISCONSIN
 BILL MCCOLLUM, FLORIDA
 GEORGE W. GELAS, PENNSYLVANIA
 HOWARD COLE, NORTH CAROLINA
 B. FRENCH BLAUGHTER, JR., VIRGINIA
 LAMAR E. SMITH, TEXAS
 CRAIG T. JAMES, FLORIDA
 TOM CAMPBELL, CALIFORNIA
 STEVEN SCHIFF, NEW MEXICO
 JIM RAMSTAD, MINNESOTA

MAJORITY—225-3061

MINORITY—225-9906

June 12, 1991

The Honorable William H. Webster
 Director
 Central Intelligence Agency
 Washington, D.C. 20505

Dear Mr. Webster:

In pursuit of our oversight responsibility regarding enforcement of the nation's drug laws, the Committee on the Judiciary, through two of its Subcommittees, has asked the General Accounting Office to collect information on automated drug enforcement information systems.

The Central Intelligence Agency operates one or more such computer systems and is also conducting its own survey of other agencies' systems parallel to the GAO study we have requested. Unfortunately, the CIA has declines to cooperate fully with the GAO, and has refused to provide sufficient information on either the Agency's own counternarcotics systems, or the results of the CIA's survey of other agencies' systems.

In a separate inquiry, the Committee has asked GAO's Office of Special Investigations to conduct a review to determine the extent to which foreign industrial and economic espionage is being conducted in the United States. As part of this investigation, we directed the GAO to contact the CIA and to arrange for a briefing on the subject. Once again, the Agency denied GAO's request.

In support of the decision by the CIA not to cooperate with the Committee and the GAO in these matters, the Director of your Office of Congressional Affairs said in recent letters that CIA information "is discussed exclusively with the Intelligence Committees of the House and Senate, in keeping with the determination of the Congress to vest by statute responsibility for intelligence oversight in these two committee[s]."

Contrary to the understanding of your Congressional Affairs Director, Congress has never stated that the jurisdiction of the intelligence committees is exclusive. Indeed, House rule XLVIII establishing the Intelligence Committee explicitly states:

"(c) Nothing in this rule shall be construed as prohibiting or otherwise restricting the authority of any other committee to study and review any intelligence or intelligence-related activity to the extent that such activity directly affects a matter otherwise within the jurisdiction of such committee.

The Honorable William H. Webster
 Page Two
 June 12, 1991

S. Res. 400 from the 94th Congress, establishing the Senate Select Committee on Intelligence, contains essentially identical language.

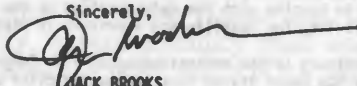
The Intelligence Oversight Act created a system of regular and comprehensive reporting to the Intelligence Committees. It did not insulate the intelligence agencies from specific requests from other committees on matters within their jurisdiction. Indeed, the Intelligence Oversight Act explicitly recognizes the jurisdiction other committees have over intelligence matters. Section 501(d) provides that each of the intelligence committees "shall promptly call to the attention of ... any appropriate committee or committees of its respective House any matter relating to intelligence activities requiring the attention of ... such committee or committees." This can only mean that such committees have authority to pursue the matters called to their attention, and there is no requirement that such committees must await a referral from the intelligence committees before exercising their jurisdiction. Nor is there any indication they must funnel all requests for information through the intelligence committees. Indeed, the House Intelligence Committee does not want to serve as a go-between for other committees' work.

The enforcement of the nation's drug laws and the potentially damaging effects of foreign economic espionage in the United States are clearly matters within the jurisdiction of the Judiciary Committee, and the Committee plans to pursue its oversight responsibilities with the assistance of the GAO. Since the CIA contributes to the drug enforcement effort and to counterespionage activities, the CIA's role in these matters is subject to the oversight of the Judiciary Committee.

I am therefore requesting that you direct the appropriate officials to cooperate with the Committee and the GAO by providing the requested information without further delay. If there are extenuating circumstances involved, I am sure the matter can be resolved in a way that meets the needs of the Judiciary Committee and the CIA. Since two important committee investigations are being held up pending the resolution of this issue, I must ask that you respond to my request by July 8, 1991.

With best wishes, I am

Sincerely,



JACK BROOKS
 Chairman

Central Intelligence Agency



JUL 16 1991

RECEIVED

JUL 22 1991

JUDICIARY COMMITTEE

16 July 1991

The Honorable Jack Brooks
Chairman
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This is in response to your recent letters regarding access by GAO and the Judiciary Committee to certain CIA information regarding automated drug enforcement information systems and foreign industrial and economic espionage in the U.S. My staff is preparing answers to questions posed in your letter of June 10 concerning drug enforcement information systems, and they will be provided to you shortly.

We do, of course, understand and support the Committee's need for intelligence information relevant to particular matters under its jurisdiction. It is not our position that intelligence information can be discussed only with the Intelligence Committees of the Congress. We provide hundreds of classified briefings and publications each year to individual Members and a variety of Congressional committees. We also provide considerable substantive intelligence support to the General Accounting Office.

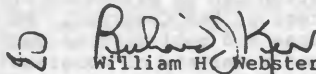
The need to provide congressional committees with information relevant to their various responsibilities should not, however, be equated with a requirement that GAO be permitted to have unlimited access to intelligence information in connection with any investigation it may conduct on behalf of a committee or individual member of Congress. Congress itself chose to limit GAO's access to intelligence information when it enacted legislation that excluded GAO from auditing CIA's unvouchered funds, and gave the President broad authority to exempt from such audit other financial transactions relating to sensitive foreign intelligence or counterintelligence activities. Congress also has denied GAO authority to enforce subpoenas or court orders for material related to activities designated by the President as being foreign intelligence or counterintelligence activities. Congress has instead specifically provided for review and oversight of intelligence activities by the House and Senate Select Committees on Intelligence.

The Honorable Jack Brooks

Your letter also raises the issue of oversight by your Committee of CIA's role in drug enforcement and counterespionage activities. We cannot agree with your view that these activities are subject to oversight by the Judiciary Committee. The legislative history of the Intelligence Oversight Act of 1980 makes clear that both the Legislative and Executive branches believed that they were establishing the comprehensive and exclusive mechanism for Congressional oversight of intelligence activities. In fact, one of the major purposes of the Intelligence Oversight Act was to reduce the number of Congressional committees having access to sensitive intelligence information. We believe your position, if carried to its logical conclusion, would allow limitless assertions of jurisdiction over intelligence activities, running directly counter to the system of oversight that the Congress created and disrupting arrangements that have served our country well.

In our view it would be far more productive for us to work together in an effort to provide direct substantive intelligence support to your Committee's efforts than to argue in the abstract about oversight jurisdiction or the role of GAO. I have instructed my staff to contact your chief counsel to pursue this goal.

Sincerely,


William H. Webster

Director of Central Intelligence

Mr. BROOKS. I would yield now to the distinguished minority leader of this committee, Mr. Fish of New York.

Mr. FISH. Thank you, Mr. Chairman.

Judge Sessions, in several areas of your testimony you state the difficulty in defining key issues, key terms such as "proprietary technology" and "economic information." Can you describe the process by which you will come to define such terms and how American business will be involved, if at all, in that process.

Mr. SESSIONS. Yes. The ability of the FBI to arrive at a uniform definition on proprietary information and applying it to the theft provisions of title 18 to ensure a uniform application and to encompass intangible information is something that we might seek. But what we are doing under the aegis of the Department of Justice is to continue those conversations to try to arrive at those definitions that will have appropriate application to our criminal responsibility and our counterintelligence responsibility, so arriving at a definition is extremely important to us.

Mr. FISH. And the role of American businesses in helping you?

Mr. SESSIONS. I'm not sure precisely what you are seeking from me in that connection.

Mr. FISH. Well, I mean how they define terms such as "proprietary technology" and "economic information." They ought to have it already, I would think.

Mr. SESSIONS. I would think that they can be of great help in bringing about a definition that will cover their needs, and if they will express those in the normal ways, I presume those will be absorbed by the Department of Justice in pursuing the creation of an appropriate definition in the legislative language.

Mr. FISH. Thank you.

Director Gates, to what extent can U.S. companies protect themselves from foreign economic espionage using current technology, and what is the CIA's role, if any, in assisting companies to use such technology to protect themselves?

Mr. GATES. Maybe I'm in a better position in deferring to my colleague from the National Security Agency on this. I think that our primary role in helping them is in our worldwide counterintelligence activity and when we can let them know that they are being targeted, and especially if we can let them know the way in which they are being targeted, whether people are trying to plant moles or simply bugging their offices or something like that.

The degree to which they can protect themselves electronically—and, again, I defer to my colleague—to a degree, I think, depends on the sophistication of the service that is attacking them. There are probably a number of services against which they can protect themselves with certainly existing technologies or capabilities that they currently have.

Against the best services in the world, a dedicated effort I think would be very difficult for them, but I think I have just exhausted my technical expertise and I had better defer to my colleague.

Mr. FISH. Dr. Hearn.

Dr. HEARN. Mr. Fish, we have no direct relationship under the Computer Security Act, which limited our activities, with U.S. industry in general, and NIST would be a better Government agency to direct that question to.

Mr. FISH. Excuse me?

Dr. HEARN. The NIST, the National Institute of Standards and Technology, has the charter to deal with the private sector in the protection of sensitive and unclassified information. As far as U.S. defense contractors are concerned working on classified contracts, that is an area where we do have oversight and influence.

Mr. FISH. Thank you.

I go back to you, Judge Sessions, in defining these business terms. What is your relationship with NIST?

Mr. SESSIONS. If I may comment on the previous question, it seems to me it is absolutely essential that the FBI continues its work with businesses that it has long pursued with agencies that use classified information in the production of their products.

We have the counterintelligence awareness briefings that we routinely have with literally thousands of businesses, and we are expanding that to include other businesses that need to have or should have a counterintelligence awareness of the activities that are being directed against their companies, and I believe that is an extremely important concept. I would not speak for the CIA, but they have, as I understand it, generally the same types of briefings that relate to those companies that do work for them.

It obviously is an area, with the economic espionage, that we will need to pay greater and greater attention to and meet the needs of those private enterprises that are suffering from, as Mr. Gates puts it, state-sponsored activity directed against them in one form or another.

Mr. FISH. But Dr. Hearn has just brought up this National Institute of Standards and Technology. How do they fit in here? Because this all goes back to this idea we started exploring earlier today about better coordination between the various agencies of Government.

Mr. SESSIONS. I think I would need to defer to Dr. Hearn.

Mr. FISH. He brought it up. You passed the buck to them, and now they are unknown to the FBI? What is going on?

Dr. HEARN. Again, under the Computer Security Act of 1987, the NIST has the charter to advise the private sector in areas of information protection. We act as NIST's technical adviser when requested by them.

Mr. GLICKMAN. Would my colleague yield on that question?

Mr. FISH. Yes, of course.

Mr. GLICKMAN. I think that statement is kind of disingenuous. That implies that the NSA has no role whatsoever in either coordinating, leading, or directing NIST as to the subject matter of Mr. Fish's question. That is just not true.

Dr. HEARN. In my remarks, Mr. Glickman, in the testimony I gave, the 5-minute summary, I highlighted several areas where we cooperated and supported NIST in the security domain. So I did not wish to appear disingenuous, and I think my remarks of the earlier session underscore that.

Mr. FISH. Would you repeat what you said the role of the NIST is.

Dr. HEARN. One of their roles under the Computer Security Act is to advise the private sector in matters of protecting sensitive, unclassified information.

Mr. FISH. Well, isn't that what we are talking about all morning?

Dr. HEARN. That has been a focus of our discussions, yes.

Mr. FISH. Well, maybe we could explore that with the next panel. But I would think that would be, Judge Sessions, an entity that would be part of your consultation.

My next question is directed to both Judge Sessions and Director Gates. Is it possible for a U.S. company to become so secure from espionage that it would be difficult also for the FBI or the CIA to detect possible illegal behavior of that company? And, if so, what safeguards can be used to protect access by law enforcement agencies where necessary?

Mr. SESSIONS. I think what you have asked underscores the importance of the ability of the FBI to have access through court-ordered interception of information. If a company had capabilities which did not accommodate the carrying out of the court order, then they might well be able to escape detection.

You will recall, Mr. Fish, that the title III wiretap is only used in the most extreme circumstances when no other method is available. It is, in a sense, a last resort mechanism, and part of our responsibility in making application to the Department of Justice for that authority and authorization is to show to the court that we have exhausted other means, other capabilities, other techniques to invade and find that and prove that criminal activity. So if they were so secure, as your question assumes, that we were not able, through electronic capabilities, to carry out our responsibility under the 1968 law where title III exists, we would maybe be foreclosed from being able to prove that criminal conduct with that company, and it is very important.

The last question that you asked, I can give you a partial answer that I should have been able to give you before, and I apologize. Mr. Gow reminds me that within the Intelligence Division there is a continuing working relationship on the threat analysis between NIST and the FBI, and I should have said that it is continuing, and I will be glad to expand it further for the record.

Mr. FISH. That is fine. Thank you very much.

Director Gates, do you have anything to add to Judge Sessions' response?

Mr. GATES. No, sir. When it comes to the possibility of wrongdoing by U.S. companies, that is the province of the FBI.

Mr. FISH. Then I have one last one for you, if the Chair will indulge me in this regard. It has been mentioned by several people this morning in various ways that part of this foreign espionage is being conducted, if I understood correctly, by republics of the former Soviet Union. Is that an accurate statement, as distinct from one republic of the former Soviet Union? I mean everybody said it several times, that they are in the business. You even tried to explain why, because they are starting from such a low base that they need to hurry up and steal what they need rather than develop it themselves.

Mr. GATES. The primary activity that we have seen, Mr. Fish, has concerned the Russian Republic. It would appear to us that most of the operations we see are continuations of operations that were under way prior to the coup attempt in August 1991.

It is not clear what the motives of some of these operations are, whether they are continuing just on bureaucratic inertia, whether there is even knowledge of them at the political level in Moscow, but we have seen them, and it is primarily the Russian Republic.

Mr. FISH. I assumed that was the case, that it was primarily the Russian Republic, because the KGB has been disbanded and the Ministry of Security created, which is located within the Russian Republic. But I can't get over this idea that it is almost as if it was countenanced as a matter of full employment for former KGB agents, that they are out there all over Europe, trying to find proprietary information from U.S. corporations to help the Russian Republic to catch up.

Now that may laudable from their point of view, but it does seem to me that we have a handle there since we are being asked to contribute quite generously to the economic and political stability of the area, particularly the Russian Republic, that we would be able to put a halt to this particular aspect of foreign espionage.

Mr. GATES. If I may, Mr. Fish, it is clear that the Russian Republic does not have the kind of oversight process that the United States of America has for its intelligence services, and, as I suggested, it may well be that the political level in Moscow does not even know that these activities are taking place. This was always, or was for many, many years, as I think Judge Sessions will attest, one of the top priorities, if not the top priority, of the KGB in the old Union, to collect technology, and there is a certain sense of this just rolling forward.

Mr. FISH. Since it has been talked about by witnesses from the General Accounting Office and this panel today, I'm sure it will come to their attention, and hopefully something can be directed to stopping it.

Thank you very much.

Mr. GLICKMAN. First of all, I want to welcome the witnesses. I guess as of today I'm the only member of this committee that is also a member of Intelligence. I know Mr. Hyde was, and there had been others in the past. So I appreciate both Mr. Sessions and Mr. Gates testifying.

Isn't the bottom line on this issue of encryption technology, digital telephony, that you all don't want the approval of technology that is so good that it will not only protect the companies from being invaded but it will protect you from getting into the information? That is, you don't mind the status quo, but you think for law enforcement purposes if the technology keeps going and the encryption keeps improving, then it is going to keep you out of the communications.

Mr. SESSIONS. What I want is what the law provides. The Congress of the United States has long since decided that there are areas of concern that overrule the right to privacy. When there is criminal conduct, the Congress has decided by title III that the FBI, among other agencies, should have an electronic capability to find that activity, so that there is no question that we must have that capability, and we went along, Mr. Chairman, for years with the analog capability and we were easily able to invade it. We pursued that in discussions with those companies to ensure that as

they went into the digital area we would continue to have access to carry out our court-ordered responsibility under the law.

When we found that that was not happening—that is, that we were not going to be assured of access either through cooperation necessarily or through legislation as it presently exists—we needed to pursue it, and we did. The Congress of the United States, I believe, wants to carry out the intent of title III, and it has intended that since 1968, and unless we have that access allowed us by those companies built into their products, we may well be denied the access.

Mr. GLICKMAN. Let me read a letter that the committee received. It is addressed to Congressman Brooks. It is written by a group of entities that includes AT&T, the American Civil Liberties Union, IBM, the Information Technology Association, Nynex, Pacific Tele- sis, and the Software Publishers, and basically it argues very strongly against the FBI's proposal regarding digital telephony. I'm going to read from one paragraph of the letter, and then I would ask that the letter be included in the record.

"This proposal would not only impede the development of digital telecommunications technology but would prohibit American businesses from installing secure communications lines for discussions of proprietary items and trade secrets. U.S. companies face a growing threat of theft of proprietary information both here and abroad. To protect themselves, American companies have sought digital systems with high levels of security. We firmly believe that any otherwise secure system which is made open to FBI surveillance would be vulnerable to others."

[The letter follows:]

PODESTA ASSOCIATES, INC.

John D. Podesta

124 C Street, NE • Washington, DC 20002 • 202 544-6906 • Fax 202 543-2361



Jerry Berman
Director, Washington Office

Electronic Frontier Foundation, Inc.
646 Pennsylvania Ave. SE, Suite 303
Washington, DC 20003
(202) 544-9237
Fax: (202) 547-5481
Internet: jberman@eff.org

Chairman
House Committee on the Judiciary
2449 Rayburn House Office Building
Washington, D.C. 20515

RECEIVED

APR 14 1992

JUDICIARY COMMITTEE

Dear Chairman Brooks:

We write out of concern over the Federal Bureau of Investigation's (FBI's) proposal regarding digital telephony. We represent a wide range of manufacturers, providers, and users of electronic communications, as well as privacy advocates. While we understand that law enforcement needs to have the capacity to execute valid warrants to seize digital communications, we are gravely concerned about the proposal put forth by the FBI. We believe that no legislative solution is necessary. The interested parties are fully cooperative and willing to work out a solution. Indeed, industry and the FBI have met and agreed to form a working committee to address the needs of law enforcement agencies for continued ability to intercept communications pursuant to a valid warrant.

The proposal would broaden the authority of the Federal Communications Commission to license telecommunications equipment and would cover not only traditional telephones and newer digital technology, but all types of computer communication, and possibly radio communication as well. The proposed legislative language is very broad and, we believe, very intrusive. It would require telecommunications and computer equipment manufacturers here and abroad to follow government guidelines in developing their products and to finance changes in their current systems to comply with the law, if enacted.

This proposal would not only impede the development of digital telecommunications technology, but prohibit American businesses from installing secure communications lines for discussions of proprietary items and trade secrets. United States' companies face a growing threat of theft of proprietary information both here and abroad. To protect themselves, American companies have sought digital systems with high levels of security. We firmly believe that any otherwise secure system which is made open to FBI surveillance would be vulnerable to others.

Any proposal to limit privacy rights of American consumers and American business users should be given very close scrutiny. At a House hearing held two weeks ago, FBI Director Sessions testified that the Bureau had not yet encountered any difficulties in executing a warrant because of digital communications. We see no need to hurry a

April 10, 1992
Page Two

legislative solution -- especially one which might seriously impair privacy and technological development -- when no problem has yet occurred. For these reasons, we hope that you will conclude, as we have, that these issues can be resolved without resort to legislation.

Sincerely,

American Association of Law Libraries

American Civil Liberties Union/ Privacy and Technology Project

Association of Research Libraries

AT&T

Cellular Telecommunications Industry Association

Computer & Business Equipment Manufacturers Association

Computer & Communications Industry Association

Computer Professionals for Social Responsibility

Digital Equipment Corporation

Electronic Frontier Foundation

Electronic Mail Association

GTE

IBM

Information Industry Association

Information Technology Association of America

Lotus Development Corporation

McCaw Cellular Communications, Inc.

Microsoft Corporation

NYNEX

Pacific Telesis Group

Software Publishers Association

Southwestern Bell Corporation

Telecommunications Industry Association

United States Telephone Association

U S WEST

Mr. GLICKMAN. Now I guess what I'm saying is, do we not have a classic public policy conflict here whereas the world is moving so quickly that folks who want to steal secrets from American companies are trying to do so, and in order to make these companies safe from that kind of theft, they almost have to make them safe from American law enforcement officials as well?

I mean I understand what you are saying, and that is that Congress has talked about wiretap statutes in order to ensure normal law enforcement, but I think we have a tremendous conflict of public policy objectives right here.

Mr. SESSIONS. Mr. Chairman, I don't think we have a conflict of policy at all. I think what Mr. Fish asked in his question about being so secure that even the FBI could not, under its proper, lawful authorization, invade those conversations or the conveyancing of information, if you took the very list of companies that you have listed and read into that context the very paragraph that you have read, it falls exactly into what Mr. Fish was talking about, the capability to have access under the laws of the United States with the safeguards and assurances that the law gives with the very careful following of title III, with all of its precise requirements, the oversight by the courts all the way up to the Supreme Court of the United States, the oversight of the Attorney General, the oversight of the committees, all these that give to the FBI the lawful authorization to invade those systems. If it is defeated by technology developed thus far, we cannot carry out our responsibility under law.

Mr. GLICKMAN. So what you are saying—now let's be honest about it.

Mr. SESSIONS. I'm trying.

Mr. GLICKMAN. I'm not saying you aren't. But what you are saying is that systems that are so secure to protect against economic threats from the rest of the world, absolutely, which also make it so you can't eavesdrop legally should not be done; that is public policy; we should not let that happen.

Mr. SESSIONS. I think that is exactly correct, and I think that is what the Congress is concerned about and should be concerned about and solved in 1968. It said, "You must have access for those purposes. Notwithstanding the Constitution of the United States, we have defined and designed a system which will allow the FBI and other agencies to interdict criminality," and if you deny that or if you say, "Well, we'll leave it to cooperation," you can imagine that the FBI would have to build another agency to actually foster cooperation, limit statutes that will allow us to have access, and those companies—pardon me, Mr. Chairman.

Mr. GLICKMAN. Yes, go ahead.

Mr. SESSIONS. Those companies, in their developmental process of these phenomenal techniques, with their knowledge of those techniques, are far able to design the capability to give the FBI access and to give that lawful access as required.

Mr. GLICKMAN. We will hear that. Let me tell you what I suspect is happening, and I don't deny—I think there is a conflict here, because I think technology has made it a conflict. But the problem is that our Government is impeding the private sector's development of modern cryptographic technologies because they don't want those technologies to get too sophisticated, whether it is the intel-

ligence agencies or whether it is the Bureau or whether it is other law enforcement people. I mean I honestly believe that.

You talk to the National Institute of Standards and Technology that Dr. Hearn referred to. I have heard from people who work in that agency who have told me the very same thing over the years.

Mr. SESSIONS. If you woke me up in the middle of the night and threatened me with the most dire of consequences, I would say that is not so. I would say that the FBI wants very much to see advancing technology, greater capabilities, greater implementation throughout the world. All we are asking is what the Congress has already given; that is, the continued lawful access.

We are involved with a great deal of our own budgeting capability in development of technologies that will allow us to carry out the law, and I do not find myself at odds with the Congress at all. I do find myself at odds with people who say, "Well, rely on cooperation." That is not what we are required to do. There are so many different companies, so many different interests, that unless we take the digital telephony and do it by statute and provide some mechanism whereby that cooperation can be fostered as well as the law followed, we are going to find ourselves without capability.

Mr. GLICKMAN. OK. I don't disagree, and I think implicit in your last statement is that you do understand there are conflicting and competing public policy interests involved. This is a mighty mean competitive world out there, and there are predators who will do anything within their power to take technology and advancement away from American business and America generally, and all these people are trying to do is to protect themselves from that. Unfortunately, they may ultimately end up protecting the system so greatly that you can't intervene either. That is the problem.

Mr. SESSIONS. There may be an additional burden on those companies to carry out their responsibility under the law of the United States, but I say that is the higher and greater good, because that is the ability that the law presumes we have and will always have; that is, to interdict criminality; and that again goes back to Mr. Fish's original scenario, and it is a real scenario, because we would be kept out.

Mr. GLICKMAN. I have no questions, but I yield to my colleague from New York.

Mr. FISH. Just on this point, because I think it has now been clarified, what is good for an American company may be bad for the FBI. So what do we do about it? I understand the concerns expressed in the letter that the chairman just read refer to proposed legislation that is pending before us that would broaden the authority of the Federal Communications Commission in this area; is that correct?

Mr. SESSIONS. Mr. Fish, it is not yet pending before you, and I presume that the Department of Justice and the Attorney General will come forward with legislation that will be effective to allow the digital telephony access that we seek. I don't believe there is legislation before you. What is before you is a proposal that somehow; that is, in this context, there is a proposal that somehow we be provided legislative relief that will allow us to not have to go back with each developing and exploding technology and seek access again. But rather that we have a mechanism whereby by the law

that the Congress has enacted can be carried out regardless of the technology.

And there is some burden on the private sector, but it is not a detrimental burden. It is, in that sense, a cost of doing business that allows the Government, where it has shown that it has a rightful place, to actually invade and have access to that information. And that is not new. It has been done before, and the burden has been placed upon industry before.

I don't look at it as impeding technology. Quite to the contrary, I simply view it as accommodating and acknowledging that need and building it into the technology.

Mr. FISH. Well, but it is a very, very heavy issue here, and I hope that in the course of seeking a response to the Congress that you would also think in terms of, perhaps, a different approach, one that would increase penalties to such a point that if companies did end up with the technology that you could not invade they would do it at such great peril—they would engage in criminal activity in such great peril that it would meet your objections.

Mr. SESSIONS. The proposal, the original proposal, which I think will not end up being the proposal, the Department of Justice contemplated that the Federal Communications Commission would have an ability to deal with it in that area; that is, through penalties for failure to do it or through other sanctions that would be effective.

But I would say that it is one of those things that the Congress must not surrender its prerogatives on. That is, the decision that was made in 1968 to actually give the title III capability is critical. It is as critical today at this moment as it was then, and the Congress ultimately will have to assume the responsibility if it fails to give us that access. And that is all we seek in the digital telephony, staving access to the technology, hopefully cooperatively.

And I think we have pursued it correctly, Mr. Fish. Last week we met again with the people from the companies in an extended session. We have met at the invitation of the Attorney General with the heads of those companies to be sure that they understood that for 3 years now we have been pursuing with the companies, with the expectation that we would be accommodated, and now we find that that digital telephony has advanced to such a point that we are nearing the point where we will be denied access on a routine basis. We have not suffered it yet.

The Congress would expect us to come back and say, "We need this capability," and to examine it carefully, and to be sure that we are not foreclosed. And I think the Congress will burden industry, if that is the correct term, with the responsibility to see that whatever technology they have, that the intent of the law is not evaded.

Mr. FISH. Thank you very much, Judge.

Mr. GLICKMAN. Let me just ask a couple of additional questions. Judge, I think it was last year the FBI reallocated some of its foreign counterintelligence people to—I think it was 425, if I am not mistaken—into areas like violent crime and health care fraud and those kinds of things. I don't remember what the exact numbers were.

I wonder if you could comment on how that would affect the kind of work you are doing in this area?

Mr. SESSIONS. I would be pleased to, Mr. Chairman. Probably it is a short question that requires a longer answer, but I will try to keep myself under control.

Back in 1989 when we first saw what happened at Tiananmen Square and had some suspicion that this kind of response of people to their urges for freedom might have impact on the rest of the world, we looked at it at the FBI and we talked about it, and we said, "How can our counterintelligence responsibility be met if that sort of thing happens?"

And sure enough, that sort of thing did happen, and our counterintelligence responsibility that was related to the attacks that were made on America either through the then Soviet Union or their surrogates began to change, and with these emerging democracies in Eastern Europe, sure enough the FBI through the NSTL—the National Security Threat List—was able to see that the activities of those surrogate countries was lessening or was ceasing entirely. And when it lessened and ceased, what we had, Mr. Chairman, was then the ability to say we have seen it. What are you going to do about it? And the answer was: Why should we wait for a particular budgetary cycle? Why should we wait for next year? What does the Congress expect us to do? It expects us to use our resources properly.

If we no longer have that burden from those countries that previously attacked us, then the philosophy was take those people and put them into other meaningful activities.

Mr. GLICKMAN. So, essentially, the people that were roughly allocated to Communist bloc countries were reallocated to domestic programs.

Mr. SESSIONS. That is a good analysis. And what happened further was the Attorney General, Mr. Barr, when we did it agreed with us that in fact if we were wrong in our estimate that we would go back and seek reprogramming back into the foreign counterintelligence responsibility. So I am very comfortable, first of all, that we are focused; second of all, that if we are wrong, and that is possible, then we will be able to recount and go back and make those corrections and meet that threat.

Mr. GLICKMAN. OK. Mr. Gates, what do you do with this problem of state-sponsored versus nonstate-sponsored foreign intelligence and other situations where, let's say, you have a country like Japan that may not have an intelligence service, at least to my knowledge. But they do have organizations of government that might be engaged in cooperative relationships with private sector companies that may hypothetically be involved in intelligence operations.

How do you deal with this issue if something isn't government-run—like if it is not the intelligence unit of the French Government, but intelligence operations of French companies? In a modern world where the governments and their companies work so closely together, how do you make the decision as to what you are going to target in terms of your own operations?

Mr. GATES. I think the key criterion is whether we can detect that a foreign government has a hand in it whether or not it is a classic intelligence organization. I have in my full statement that was submitted for the record the example of a researcher who comes from a foreign country to the United States to attend a con-

ference and goes around and elicits information. What is of interest to us is was that person sent? Was that person given a list of collection requirements? Was that person targeted against specific individuals?

We don't have to go against an intelligence organization necessarily to find out the answers to those questions. We can try and find the answers to those questions through the activities of other elements of those governments. So we are not limited—I do not consider us limited to classic intelligence services, as it were.

Mr. GLICKMAN. And would you agree with that, Judge Sessions?

Mr. SESSIONS. I would. And what he has pointed out is very significant. It is in the art of counterintelligence that you can find out those things about the thrust of what that person is doing, and we must be certain in our requirement that it is state-sponsored, that it is in some way tied there, otherwise we have no ability to track him.

Mr. GLICKMAN. But you may have nonstate-sponsored in a classical sense, but a wink and a nod by the state agencies. And even they may not be classic intelligence agencies. They may be their agency of commerce or other kinds of agencies. I just want to make sure that our intelligence—counterintelligence operations are flexible enough to deal with that.

Mr. GATES. That is why I think, Mr. Chairman, that the different elements of our work on economic intelligence are interrelated. In other words, to the degree that we consider and have been tasked by our policy community to identify the ways in which governments go about conducting economic policy and the division of labor in foreign governments and how they do business, this is the way in which we gain a window into the kinds of activities that you have identified and that in some respects are gray areas. It is through this larger aspect of looking at the way people do business.

Mr. GLICKMAN. Let me ask two more questions. On page 16 of your statement, Mr. Gates, you indicate something that is kind of scary to me. You talk about in a third pattern the intelligence service of a foreign government conducts bag operations within its own border, surreptitiously entering hotel rooms of visiting American officials or executives to search for documents containing sensitive economic or business data, taking advantage of other security lapses as well, and passing the information gathered to national firms.

Tell me about the prevalence, if you can, in a generic sense of that kind of thing. Should American businessmen or women who are traveling overseas take extra security precautions when they are traveling concerning the viability of the information they are containing with them? Should they be careful not to keep information in hotel rooms? Are hotel rooms routinely broken into, I mean? Are they eavesdropped upon?

I want to know what the nature of this problem is.

Mr. GATES. It clearly varies from country to country, Mr. Chairman, but my general advice would be that yes, they should take measures to protect against that kind of thing. If they are carrying information that is sensitive in terms of either company technology or negotiations or something of that sort, I think that taking some

measures to protect that information, not leaving it unattended, would be only prudent.

Mr. GLICKMAN. And they should expect that it is indeed within the realm of possibility that their privacy will be invaded and the information will be copied, or at least reviewed?

Mr. GATES. Again, it varies from country to country, and as I have indicated, when we know a company is being targeted we will tell them so or find a way to get that information to them. But I think that again within the realm of all the possibilities being cautious makes a lot of sense.

Mr. GLICKMAN. And do you tip off firms that are hit by foreign spying, either you or the FBI? Will you give that information to companies?

Mr. GATES. When we have information that a specific company is being targeted by a foreign government or a foreign intelligence service, yes, we will. We will find a way, either through the FBI or directly, whether specific or generic, to try and let them know that they are at risk.

Mr. GLICKMAN. Judge Sessions.

Mr. SESSIONS. What you have asked and what Mr. Gates has answered falls classically into the realm of counterintelligence awareness. I think he is absolutely correct where a company has a strong interest in the sanctity of that information it needs to be aware and take steps to ensure that that is not taken away from them, and the simplest measures fall, or follow on the counterintelligence awareness. That is, somebody else wants what I have got. This information is critical to us, therefore protect it.

Mr. GLICKMAN. I think we are finished. We thank you all very much for testifying today. We appreciate it very much.

Mr. SESSIONS. Thank you for the opportunity, Mr. Chairman.

Mr. GATES. Thank you, Mr. Chairman.

Mr. GLICKMAN. You are welcome.

[Response to Mr. Brooks' questions for the record follow:]

MR. BROOKS' QUESTIONS FOR THE RECORD FOR MR. SESSIONS

Please provide a copy of any studies or papers sent to the House Intelligence Committee regarding economic espionage.



U.S. Department of Justice

Federal Bureau of Investigation

MAY 27 1992

Washington, D.C. 20535

May 20, 1992

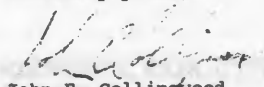
Honorable Jack Brooks
Chairman
Subcommittee on Economic
and Commercial Law
Committee on the Judiciary
Washington, D.C.

Dear Mr. Chairman:

By memorandum of May 11th, you requested that the FBI provide copies of any studies or papers sent to the Permanent Select Committee on Intelligence regarding economic espionage. This material would be included in the record of the April 29th Subcommittee hearing on Economic Espionage. Because the FBI has not provided any such information to the Permanent Select Committee on Intelligence, we have nothing for addition to the hearing record.

Please let me know whenever we may be of further assistance.

Sincerely yours,


John E. Collingwood
Inspector in Charge
Congressional Affairs Office



MR. BROOKS' QUESTIONS FOR THE RECORD FOR MR. GATES**Question**

Please provide National Security Directive #68 and National Security Review # 29 which related to the presidential ordered reassessment of the intelligence community. Please include in your response all studies, assessments, and reports conducted under NSD #68 and NSR #29 including all policy changes, recommendations, findings and conclusions.

Answer

National Security Directive #68 and National Security Review #29 are National Security Council documents. We must direct the Committee's request for those, and related, documents to the National Security Council.

MR. BROOKS' QUESTION FOR THE RECORD FOR DR. HEARN

Question. Do you plan to support the Digital Encryption Standard when it comes up for renewal in January 1993? If not, why?

Answer. NSA does not currently have any plans regarding the renewal of DES in 1993. If NIST requests NSA's help, NSA technical experts will fully examine the algorithms and the security it should provide and will render the algorithm and the security it should provide and will render their best judgment on whether or not to recommend renewal.

Mr. GLICKMAN. We have a last panel—I have it somewhere here.
[Pause]

Mr. GLICKMAN. We will now hear from our witnesses on the final panel: Mr. Riesbeck, Mr. Phelps, and Mr. Levchenko.

James E. Riesbeck is executive vice president for Corning Inc. He joined Corning in 1966. He has held the position of executive vice president and member of the management committee since December 1989.

Marshall Phelps, Jr., joined IBM in 1971 and has held various positions in the corporation. Just prior to his present position, he was director for government affairs here in Washington, and last month he was promoted to vice president of IBM for commercial and industry relations.

Finally, our third witness is Stanislav Levchenko. He is a former KGB official who defected to the United States in 1979 after becoming disenchanted with the Soviet Union. He is not from the current crop of ex-KGB agents who will talk to anyone for a buck—or for cash. These are Mr. Brooks' characterizations. When Mr. Levchenko defected, I am told, the Soviet Government ordered his assassination. Mr. Levchenko, who became a U.S. citizen in 1989, is an acknowledged expert in the field of economic espionage.

Gentlemen, we appreciate your taking the time to be with us this morning. We will start with Mr. Riesbeck. Then Mr. Phelps. And finally, Mr. Levchenko.

Let me point out your entire statements will appear in the record, so you need not feel compelled to read everything you have submitted to us.

Mr. Riesbeck.

**STATEMENT OF JAMES E. RIESBECK, EXECUTIVE VICE
PRESIDENT, CORNING, INC.**

Mr. RIESBECK. Thank you. With your permission, I will summarize my written testimony which has been submitted for the record.

I commend the chairman and other members of the committee for their leadership on this issue. Corning is very concerned about the security of its trade secrets and proprietary information. The basic technology to produce glass is spread throughout the world. The competitive edge for Corning is often our capability to take basic technologies, refine and expand them to develop new and higher value-added specialty products. Once developed, we must aggressively protect our properties through intellectual property protection and corporate security.

We operate research centers on three continents. We maintain a worldwide staff covering many scientific and technical disciplines. We will remain competitive by continuing to stay on the cutting edge of technological development. We also must make sure that our technology is not stolen by international competitors.

Obviously, Corning's patents can be protected under U.S. patent law. We have made considerable use of such protection with a large degree of success. But intellectual property laws cannot protect all forms of critical business information. Trade secrets and business proprietary data must also be protected.

In some cases, the success or failure of a business is dependent upon preservation of valuable trade secrets. Corning has had a high degree of success safeguarding our domestic operations. We have, however, encountered problems abroad, particularly in Europe. Corning has been the target of state-sponsored industrial espionage aimed at our fiber optic technology.

It is important for the committee to understand that state-sponsored industrial espionage is occurring in the international business community. It is very difficult for an individual corporation to counteract this activity. The resources of any corporation are no match for industrial espionage that is sanctioned and supported by foreign governments.

We try to provide our own security by spending more money on security systems and by training individuals. But, as we increase the use of public-switched networks to transmit business proprietary information among our global locations, we face a significant new challenge in securing those communications.

Using enhanced telecommunications services to improve our efficiency is critical to our competitiveness. It is, however, also critical to us that these services such as teleconferencing be designed to ensure protection of our information. For example, if we can conduct secure teleconferences, we can reduce the need for company officials to personally carry sensitive corporate documents when abroad.

As we enter the next century, every company will be using enhanced telecommunications services provided through a public-switched network. To fail to do so will be a tremendous handicap as we seek to compete globally. Japan is implementing a plan to have in place by the year 2015 a broadband telecommunications network which will interconnect every business, school, and home in Japan. Europe is also ahead of the United States in several critical areas. Therefore, delaying implementation of enhanced telecommunications services in the name of enhanced security is not a sound option. Rather, our challenge is to also put in place an enhanced security system as an integral part of the enhanced telecommunications systems.

A public/private partnership is essential to ensure appropriate safeguards. As part of this partnership, American business has an important role.

First, business must adopt modern techniques to protect the security of physical operations and to protect the security of information transmitted over the public-switched network. Encryption devices and other security measures must be implemented globally to be effective.

Second, corporations must make their employees aware of the risks associated with economic espionage so that they build constant caution into the way they conduct their business relations. But the Government also must play a key role. Our intelligence agencies must become partners with U.S. industry in providing for

secure enhanced telecommunications services on an international basis. We need their help in facilitating the rapid deployment of encryption and other secure technologies to ensure protection of our information. Government regulations should be designed to accelerate, rather than impede, advancement of national secure telecommunications systems.

Another short-term option might be for Government agencies to consider establishing a secure overseas pipeline for use by businesses seeking to communicate proprietary information to their foreign operations. The agencies must also help us monitor significant international information technology developments. They must help protect our economy against those who do not play by the rules.

As we enter the 21st century, the United States must make it a high priority to communicate in no uncertain terms that industrial espionage is unacceptable behavior. The penalties for the practice of economic espionage either by a foreign competitor or U.S. citizen should be stiff and severe.

A counter-industrial-espionage effort by the U.S. Government on behalf of U.S. corporations is not an appropriate response. It can only encourage more unacceptable behavior. I would in this case define this counter-industrial-espionage effort as being we are not interested in counter-industrial-espionage efforts to gather information from foreign companies for our benefit. We are very much interested in counter-industrial-espionage efforts which protect us against such invasion.

Our energies must be dedicated to securing agreement on some internationally acceptable rules that are supported by a secure commercial communications system designed in cooperation with the Government.

Thank you.

[The prepared statement of Mr. Riesbeck follows:]

STATEMENT BY J.E. RIESBECK
EXECUTIVE VICE PRESIDENT
CORNING INCORPORATED
BEFORE THE
SUBCOMMITTEE ON ECONOMIC AND COMMERCIAL LAW
HOUSE JUDICIARY COMMITTEE

APRIL 29, 1992

My name is James Riesbeck. I am Executive Vice President of Corning Incorporated. I am pleased to appear before you today to provide you with the perspective of Corning Incorporated on economic espionage.

At the outset, I want to commend the Chairman and other members of the committee for their leadership on this issue. With the Cold War behind us, we must refocus national attention to our foremost challenge -- international economic competition.

For the first time since the 1930s, the United States is not threatened by a foreign military power. As a result, our stature in the world will increasingly be determined by what is done in corporate boardrooms and on factory floors, rather than by the Joint Chiefs of Staff. The priorities of our national intelligence apparatus must reflect this changing circumstance by placing greater emphasis on economic security. It is no surprise that a recent study undertaken by CIA Director Robert Gates found that the most important challenges through and beyond the end of this decade are in the international economic arena.¹

Corning is very concerned about the security of its trade secrets and business proprietary information. My testimony will include three points:

- o a description of the importance of the security of Corning's intellectual property, trade secrets, and business proprietary information to its long-term business strategy;
- o a description of the problems Corning has encountered and solutions it has adopted; and
- o a suggested public policy response to the problem.

¹"U.S. Demands for Economic Intelligence Up Sharply, Gates Says", Washington Post, April 14, 1992, p. A5.

WHY CORNING IS CONCERNED

Corning is in a business that's 4,000 years old. The Egyptians made glass. The basic technology to produce glass is highly diffused in our world. Nearly every nation already is or could be in the glass business in very short order. The competitive edge for Corning has been and always will be our capacity to take this mature basic glass-making manufacturing process and refine it to develop new and higher value added specialty products and processes. Once developed, we have sought to protect these developments aggressively through intellectual property protection and corporate security.

This competitiveness strategy based on core technology dates back to Corning's early beginnings. In 1908, we were one of the first American corporations to establish a fully dedicated corporate R&D facility. We have an enduring commitment to technology. We operate research centers on three continents, maintaining a worldwide staff covering virtually every scientific and technical discipline. Corning has historically committed five percent of sales to fund research throughout its business cycles, a rate far above the national industrial average.

Because of this commitment to R&D, Corning has many inventions to its credit, several of which have proved fundamental to our national well-being. These include:

- o the process for making glass blanks for the first electric light bulb;
- o the process for making glass for televisions;
- o development of the Celcor substrate, the ceramic core of the catalytic converter used to control environmentally damaging emissions from automobiles; and
- o the process for making fiber optics, thin strands of glass that are replacing copper as the predominant medium for telecommunications.

In addition to these fundamental inventions, Corning has a number of other principal inventions to its credit, including silicone, photochromic lenses, and specialty ceramics for space exploration.

Preserving the integrity of Corning research and development efforts is critical to the continued success of our corporation. We will survive and remain competitive by continuing to stay on the cutting edge of technological development. We must make sure that our technology is not knowingly or unknowingly stolen by our

international competitors.

THE PROBLEM

Obviously, Corning's product and process patents can be protected under U.S. patent law. We have made extensive use of such protection with a considerable amount of success. When a domestic competitor violates a Corning patent, we have recourse under U.S. patent law. When a foreign competitor violates a Corning patent and then attempts to sell goods in the U.S. market which were produced utilizing our product or process patents, we have additional protection under Section 337 of our trade laws. At times, judicial relief through the courts and administrative action through the International Trade Commission under Section 337 have been critical to preserving the integrity of our patents. A primary example of the importance of this is with fiber optics. Since originally developing this technology, we have defended it at least four times against infringement by a foreign manufacturer.

Protection of intellectual property in the U.S. market is not enough. It is increasingly important that we build on the intellectual property protection available domestically by seeking similar effective and adequate protection overseas. Such efforts are now underway in the Uruguay Round of trade negotiations.

But, intellectual property laws cannot protect all forms of critical business information. Trade secrets and business proprietary data must also be protected. Corning has many trade secrets that are absolutely critical to our continued success. In some cases, the success or failure of a business is dependent on preservation of our valuable trade secrets. The multinational character of our global operations makes it increasingly challenging to safeguard these operations.

Corning has had a high degree of success safeguarding our domestic operations. When we have encountered difficulties in the United States, state uniform trade secrets statutes have been effective.

We have, however, encountered problems abroad, particularly in Europe. Corning has been the target of state-sponsored industrial espionage efforts aimed at our fiber optic technology. It is important for the committee to understand that state-sponsored industrial espionage activity is occurring in the international business community. It is very difficult for an individual corporation to counteract this activity. The resources of a corporation -- even a large one such as Corning -- are no match for industrial espionage activities that are sanctioned and supported by foreign governments.

- 4 -

Because of these problems, we have done a lot internally to protect our own security, including spending more money on security systems and training of individuals. Nevertheless, we expect the problem to get worse over time, particularly if we do not take adequate steps to secure corporate communications when we use public switched networks to transmit business proprietary information among Corning's dispersed global locations.

Using enhanced telecommunications services to improve efficiency is absolutely critical to our long-term competitiveness. For example, through the use of video conferencing, we are able to save travel expenses and reduce time commitments in our fiber optics business. The marketing and engineering resources are located in Corning, New York and our manufacturing facility is in Wilmington, North Carolina.

Enhanced telecommunications can also be part of the solution to more secure corporate communications. If we can conduct secure teleconferences, for example, corporate officers can minimize personal exposure abroad involving sensitive corporate documents or information.

Corning is not the only company that will be using the public switched network to enhance its efficiency and its security. In fact, a recent study by the Hudson Institute found that deploying a broadband network to enhance our communications capability nationally is the most critical thing we could do as a nation to enhance our competitiveness. In another study, the Economic Strategy Institute found that the U.S. economy could gain between \$194 billion and \$321 billion in net new GNP and between 0.2 percent and 0.4 percent in annual productivity growth if we invest in broadband telecommunications networks.

SUGGESTED RESPONSES

As we enter the next century, every company will be using enhanced telecommunications services provided through a public switched network. To fail to do so will be a tremendous handicap as we seek to compete globally in the 21st Century. Japan is implementing a plan to have in place a broadband telecommunications network which will interconnect every business, school, and home in Japan by 2015. Europe is proceeding apace as well and is ahead of the United States in several critical areas. Therefore, delaying implementation of enhanced telecommunications services in the name of enhanced security is not an option for our future. Rather, our challenge is also to put in place an enhanced security system as a complement to our enhanced telecommunications system.

We face new challenges to our corporate security problem. It is important that as the network is designed, mechanisms are built

- 5 -

into the system to provide maximum security for these communications. A public-private partnership is essential to insure appropriate safeguards.

American business has to do everything within its power to protect its own business proprietary information. This requires the adoption of modern techniques to protect both the security of physical operations and the security of information transmitted over the public switch network. Corporations must take aggressive steps to make their employees aware of the risks associated with economic espionage so that they build constant caution into the way they conduct their business relations.

But the Government also has a role. Encryption devices and other security measures must be implemented globally to be effective. The federal government should work to facilitate rapid deployment of security devices by multinational corporations in the United States and at their overseas operations. Domestic or foreign barriers to expanded use of security devices should be identified and eliminated.

Our intelligence agencies of the government must become full participants in, not obstacles to, this public-private partnership. The role these agencies play in the future will be much different than it has been in the past. Adoption of inflexible government regulations which inhibit technological progress will be damaging to U.S. competitiveness. Rather, the intelligence agencies of the future must be more involved in charting our national economic destiny, monitoring significant international technological developments, and conducting counter intelligence to help protect our economy from those who do not play by the rules. These are the three recommendations identified in the recent CIA study which I believe are right on target.²

In a sense, the challenge before us is to achieve the highest possible security level in the private sector, just as we have done in the government. The government must keep increased pressure on foreign governments, both bilaterally and multilaterally, to strengthen their regimes of intellectual property protection. Ultimately, the solution to this problem lies in internationally defined rules of the game supported by technology which make espionage a very difficult undertaking. Until that international consensus is achieved and implemented, government agencies should consider establishing a secure overseas pipeline for use by businesses seeking to communicate proprietary information to their foreign operations.

²Ibid.

CONCLUSION

As we enter the international economic competition of the 21st century, the United States must make it a high priority to communicate in no uncertain terms that industrial espionage is unacceptable behavior. The penalties for the practice of economic espionage either by a foreign competitor or a U.S. citizen should be stiff and severe. A counter industrial espionage effort by the United States government on behalf of U.S. corporations is not an appropriate response. It can only encourage more unacceptable behavior. Our energies, rather, must be dedicated to securing agreement on internationally acceptable rules of the game that are supported by a secure commercial communications system designed in cooperation with the government.

Mr. GLICKMAN. Mr. Phelps.

**STATEMENT OF MARSHALL C. PHELPS, JR., VICE PRESIDENT,
COMMERCIAL AND INDUSTRY RELATIONS, IBM CORP.**

Mr. PHELPS. This, too, will be a summary of what is in the written record.

Mr. Chairman and members of the subcommittee, you have asked us to address issues relating to IBM's experiences involving theft of our intellectual property, the Digital Signature Standard, and the Data Encryption Standard. I would like to address these in the context of their impact on the competitiveness of the industry.

The theft of corporate proprietary assets is an important issue for our company. Such theft has occurred from many quarters: Competitors, governments seeking to bolster national industrial champions, even employees. We have been the target of each.

These activities have resulted in losses to IBM in the billions.

Mr. GLICKMAN. Let me stop you there.

Mr. PHELPS. Yes.

Mr. GLICKMAN. Would you repeat that sentence for the record?

Mr. PHELPS. Sure.

Mr. GLICKMAN. These losses. These activities.

Mr. PHELPS. Yes. These activities have resulted in losses to IBM in the billions.

Mr. GLICKMAN. In the billions of dollars.

Mr. PHELPS. Settlement agreements, judicial mandates, and commitments to third parties preclude us from discussing the specifics of many of these cases, which include the theft of personal computer related technologies, theft of trade secrets critical to our mainframe systems, theft of information by governments for their own use and by their indigenous computer hardware and software suppliers, and counterfeiting of our trademark on hardware and software.

But beyond such blatant actions there is a more subtle activity aimed at undermining our industry's greatest and most competitive intellectual asset, and that is computer software. Today, the U.S. computer software and services sector leads the world in skill, investment, and market share. U.S. industry holds over 60 percent of the world market, already accounting for more than \$63 billion annually. This market, projected to reach a quarter trillion dollars by the end of the decade, outpaces all other opportunities for growth. Some of our rivals recognize these facts and are out to catch up.

There are two formulas companies can follow. One, in the words made famous by John Houseman, is the old-fashioned way. They earn it: They invest, their employees work hard, they gain experience, and they apply their creativity. Others, however, looking for a shortcut, are unwilling to rely on investment. They argue that creativity and competition are stifled by laws such as those in the United States which protect computer software. They advocate weakening those laws. The success of America's software industry demonstrates this to be an empty argument.

Hidden in the debate over the fine details of intellectual property law, the objectives of the agents of change are plain and simple. It

is about money and markets. There is but one reason to weaken U.S. laws protecting computer programs and but one reason to stand in the way of adopting similar regimes in international forums, and that is to legalize the copying of computer program expression which under present U.S. law is illegal.

The U.S. Government has done an outstanding job in bilateral and multilateral negotiations aimed at ensuring protection of intellectual property worldwide. Those efforts will soon need to be applied here at home. A concerted lobbying campaign will get underway in the United States shortly, paralleling efforts already underway abroad, to convince Congress to change U.S. laws protecting computer software. We hope this committee will be vigilant and view the arguments with the gravest suspicion.

You have also asked us to touch on the Digital Signature Standard, or DSS, an encryption technology used to verify the authenticity of signatures provided electronically. The recent draft DSS issued by the U.S. Government, unfortunately, uses a different and unproven methodology rather than relying on an internationally accepted standard for digital signature encryption.

This approach will require manufacturers and vendors to market multiple devices to meet the international standard and DSS, and, of course, users will be forced to buy multiple products. Such an approach is inefficient and avoidable through the U.S. Government's adoption of an already acceptable and accepted international standard.

Beyond DSS you have asked us to address issues surrounding the use and export of encryption technologies. For encryption to be effective and trusted, it must be available internationally and conform to international standards. The Data Encryption Standard, something called DES, has been a U.S. Government standard since 1977 and has withstood the test of time. It has the confidence of Government and private sector users worldwide, and we believe it should therefore be recertified as a Federal standard in January 1993.

The Government has legitimate concerns regarding the use of encryption technologies to facilitate criminal activity or undermine U.S. national security. We understand that. But, in formulating policy in this area, it is essential that the Government recognize the lawful uses of encryption technology as well as the offerings of comparable products by non-U.S. firms in the global market. In short, we need a balance.

Given this, we are very pleased that the congressionally created Computer Systems Security and Privacy Advisory Board recently passed a resolution calling for a national public review of the positive and negative implications surrounding the widespread use of encryption. We intend to fully participate in that review.

Thank you very much, Mr. Chairman.

Mr. GLICKMAN. Thank you.

[The prepared statement of Mr. Phelps follows:]

STATEMENT OF
MARSHALL C. PHELPS, JR.
IBM VICE PRESIDENT,
COMMERCIAL AND INDUSTRY RELATIONS
BEFORE THE
JUDICIARY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES
APRIL 29, 1992

My name is Marshall Phelps, IBM Vice President of Commercial and Industry Relations. My organization is responsible for a range of programs related to the protection and licensing of IBM's intellectual property, our business relationships with third parties, and our worldwide standards and data security activities.

You have asked me to address issues related to IBM's experiences involving theft of our intellectual property; the Digital Signature Standard (DSS); and the Data Encryption Standard (DES). I would like to address these matters in the context of their impact on the competitiveness of our industry.

This committee is well acquainted with the issue of competitiveness through its efforts to help strengthen our country's high technology industries. In particular, Chairman Brooks, we would like to thank you for your leadership and vision on early action to encourage production joint ventures. We understand the Senate has recently passed this important legislation, and we are hopeful House action will occur soon.

The U.S. computer industry employs 600,000 workers who produce more than \$165 billion in hardware, software and services annually. The industry is taking strong steps to improve its ability to compete. We are confident that America's high technology industries possess the will, talent and initiative to achieve competitive success.

But doing so will require increased attention to market requirements; continued focus on incrementally improving products to enhance their function and market appeal; improved linkages between research, development, manufacturing and marketing activities within a company and increased quality in all aspects of business.

These steps alone, however, will be undermined if our competitors engage in unfair or illegal actions.

Among the most blatant actions are outright theft of corporate proprietary assets. Such theft has occurred from many quarters: competitors, governments seeking to bolster national industrial champions, even employees. Unfortunately, IBM has been the victim of such acts.

These activities, some of which have been reported in the press, have resulted in losses to IBM in the billions. Settlement agreements, judicial mandates and commitments to third parties

including the U.S. government, preclude us from discussing the specifics of many of these cases. These examples, however, are illustrative of the scope of the problem:

-- One of the critical IBM proprietary elements of our Personal Computer (PC) technology is software known as the Basic Input/Output System, or BIOS. The BIOS controls key hardware operations, such as interactions between the computer and diskette drives, fixed disk drives, and the keyboard. This copyrighted software has been deliberately and repetitively misappropriated by many domestic and foreign companies seeking to manufacture inexpensive copies -- or clones -- of the IBM PC.

IBM has vigorously pursued these infringements, but differences in the application and enforcement of intellectual property laws around the world have frequently left us with inadequate remedies. This is one example of why we strongly support an effective intellectual property agreement as part of any acceptable GATT Uruguay Round agreement. Our expectation is that such an agreement would significantly raise the level and enforcement of laws protecting intellectual property worldwide.

-- In the 1980s, certain foreign companies engaged in activities to steal trade secret design information critical to IBM's mainframe computer systems, as well as activities

to systematically copy the software that controls those systems. We discovered these activities but, once again, to the extent the activities took place outside the U.S., we found deficiencies in some foreign laws to be an impediment to bringing corrective litigation, particularly with regard to software.

-- Over the past few years, we have found that agents of foreign governments have attempted to obtain IBM proprietary information from time to time for their use and the use of indigenous computer hardware and software suppliers.

-- And, of course, we find that problems of counterfeiting of hardware and piracy of software -- endemic to certain parts of the world -- continue to deprive us of revenues abroad and in the U.S. where pirated products are marketed that unlawfully bear our trademark.

While I am not able to go into detail on these issues due to the legal constraints I mentioned earlier, these examples give some idea of the range of the problems we face in protecting our corporate assets.

But, beyond such blatant actions, there are more subtle activities aimed at undermining the U.S. computer industry's greatest and most competitive intellectual asset -- computer software.

Today, the U.S. computer software and services sector leads the world in skill, investment and marketshare. U.S. industry holds more than 60% of the world market, already accounting for more than \$63 billion annually. With the software and services market projected to reach a quarter trillion dollars by the end of the decade, this area outpaces all other opportunities for growth in our industry. Some of our rivals recognize these facts, and are out to catch up.

There are two formulas companies can follow to advance their market share in software. One, in the words made famous by John Houseman, is the old-fashioned way; "They earn it." They invest, their employees work hard, gain expertise and apply their creativity. Success is achieved provided the product meets a market need, is superior in price and performance to products with which it competes, and is adequately and effectively protected by intellectual property laws.

It is no accident that the U.S. leads the world in this business area. Thousands of U.S. software companies are flourishing under the U.S. legal regime.

However, some competitors, looking for a short cut, are unwilling to rely on investment. Thus, in forums like the GATT intellectual property negotiations, the World Intellectual Property Organization protocol discussions, in national debates such as those surrounding the European Community software

directive, and in bilateral negotiations, these competitors -- sometimes assisted by their governments -- have lobbied to weaken the laws protecting computer programs. They argue that creativity and competition is stifled by laws such as those in place in the U.S. The success of America's software industry demonstrates this is an empty argument.

Hidden in debate over the fine details of intellectual property law, the objective of the lobbyists for change is plain and simple. It is about money and markets. At bottom, there is but one reason to amend U.S. laws protecting computer programs, and but one reason to stand in the way of adopting a similar regime in international forums. That reason is to legalize the copying of computer program expression which, under present U.S. law, is illegal to copy. Competitors seeking such a result would thereby achieve a faster and cheaper means to gain marketshare; they could simply steal the assets resulting from the creativity and ingenuity of others.

This is a subject of survival for many U.S. companies. For example, IBM currently invests about one-third of its R&D budget on software technologies and products. Many of the thousands of smaller software companies in the U.S. invest as much as 25% of their gross revenues in software R&D. Laws that permit a return on such investments are, therefore, essential to provide continued incentive to advance these technologies.

While the U.S. government has done an outstanding job in bilateral and multilateral negotiations aimed at ensuring adequate and effective protection of intellectual property worldwide, those efforts will soon need to be applied here at home. A concerted lobbying campaign will soon get underway in the U.S., paralleling efforts already underway abroad, to convince Congress to change U.S. laws protecting computer programs.

I hope that this Committee will be vigilant and view the arguments that are advanced with the gravest suspicion. Success of the U.S. industry is proof that those who would benefit from change would likely not be the large majority of companies willing to "do it the old fashioned way." Rather, the benefits would flow to those seeking to undermine our investments.

Beyond software, there is another issue which you have asked me to touch on which also affects the global competitiveness of our industry. Here, it is not foreign competitors that are hurting us, but rather our own well-intentioned government.

First, you have asked me to touch on the Digital Signature Standard, or DSS, an encryption technology used to verify the authenticity of signatures provided through electronic means. Business will continue to make use of electronic signatures instead of exchanging paper documents. The recent draft DSS issued by the U.S. government unfortunately uses a different and

unproven methodology, rather than relying on an internationally accepted standard for digital signature encryption.

The result of this approach will require vendors to design multiple devices to meet both the international standard and the DSS. Moreover, users will be forced to buy multiple products to implement the differing encryption methodologies. Such an approach is both inefficient, and avoidable through U.S. government adoption of an already accepted international standard.

Beyond DSS, you have also asked me to address issues surrounding the use and export of encryption technologies.

Our customers around the world need to ensure the security and integrity of transmitted information. One of the most accepted, and widely used, means to achieve this requirement is the use of encryption. IBM uses encryption in many of our internal systems, and some of our largest customers -- particularly in the financial community -- depend on it for a majority of their global business transactions which increasingly are conducted through global data networks.

For encryption to be effective and trusted, it must be available internationally and conform to international standards. The Data Encryption Standard (DES), which has been a U.S. government standard since 1977, has passed the test of time and has the

confidence of government and private sector users worldwide. It should, therefore, be recertified as a federal standard in January, 1993.

But even with such recertification, the existence of severe U.S. export control on DES devices will continue to harm the competitiveness of U.S. industry.

The government has legitimate concerns regarding the use of encryption technologies to facilitate criminal activity or undermine U.S. national security. We understand that. But in formulating policy in this important area, it is essential that the government recognize the lawful uses of encryption technologies as well as the offerings of comparable products by non-U.S. firms on the global market.

Restricting U.S. firms from meeting worldwide customer requirements, only to have foreign competitors meet those needs, will erode U.S. industry. A better balance of industrial interests and government requirements must be achieved, especially if industrial competitiveness is the key element of our future national security.

We are very pleased that the Congressionally created Computer Systems Security and Privacy Advisory Board recently passed a resolution calling for a national public review of the positive

and negative implications surrounding the widespread use of encryption. We intend to participate fully in this review.

In summary, the government -- all branches -- can help the computer industry become more competitive. It can do so by promoting:

- Adequate and effective legal regimes worldwide
- Vigilant enforcement of those laws
- An open international trade environment

Thank you for the opportunity to provide our views on some of the exposures affecting our global competitiveness.

Mr. GLICKMAN. Mr. Levchenko, it is a pleasure to have you here today. If you would speak into the microphone. Turn the thing on so we can hear you. We are delighted that you are here.

STATEMENT OF STANISLAV LEVCHENKO

Mr. LEVCHENKO. Thank you, Mr. Chairman. Mr. Chairman and members of the subcommittee, I will make just a very short statement. However, I think the problem I am going to cover is potentially quite important.

I am here today to discuss the threat of foreign intelligence agencies conducting economic and industrial espionage against U.S. industry. Starting in the 1960's, I began working as a specialist on Asia for the fronts of the Soviet Communist Party and the KGB. In the mid-1960's, I was ordered to become a reserve intelligence officer with the GRU, the Soviet Military Intelligence Service.

In the early 1970's I was recruited as a KGB external intelligence officer. Later, I went to Japan where a part of my responsibilities included recruiting agents in the Japanese Government, political parties and the mass media, and planting and spreading false information that was beneficial to the Soviet foreign policy goals, and also planting forgeries of foreign government documents.

Since my defection for political reasons in 1979 to the United States, I kept a close watch on the new developments in Soviet industrial intelligence. I have published three books, as well as many articles on the KGB. My testimony today is based on many years of experience in the Soviet intelligence as well as ongoing research.

As you know, after the attempted coup last August the KGB underwent, and continues to undergo, a major transformation. In place of the KGB the Ministry of Security was established. Part of its role, foreign counterintelligence, allegedly has not been reduced. The remnants of the secret police are also still there.

Only one part of the former KGB did not experience substantial cuts or restructuring—the elite former First Chief Directorate, now an independent organization called the Foreign Intelligence Service of Russia. However, its priorities have changed. Several times last year some Soviet officials indicated in interviews through the Russian media that their intelligence had changed its focus from collecting political and military information to economic and industrial information.

For decades political intelligence was the number one priority. Now, high tech industrial and economic intelligence is the most important priority of the headquarters and of the residences abroad. The economic situation of Russia and the surrounding states is severe. They do not have the resources nor the time for expensive research and development efforts necessary to compete in international markets. To survive, they will steal the proprietary secrets of foreign companies.

Within the last few weeks, France, Belgium, and the Netherlands have broken up industrial espionage rings operating on Moscow's behalf. In my view these cases reveal increased Russian industrial espionage. One typical Russian intelligence operation today would involve a Russian businessman somewhere in Russia, in Moscow, trying to start a joint venture with a U.S. company. Russian intelligence can get the cooperation of Russian business-

men by offering them help in cutting through the redtape involved in starting a joint venture. In exchange for such help the Russian businessman agrees to employ a Russian intelligence operative inside the company. In some cases U.S. citizens may be recruited as agents by the Russians. Thus, Russian intelligence will get hundreds of new covers for its operatives.

Before major restructuring of the KGB last year it assigned undercover officers to every Soviet ministry or organization involved in trading with the West. Most deputy chiefs of directorates and departments in the Ministry of Foreign Trade were, and most likely still are, intelligence officers. Russian intelligence scrutinizes most contracts signed by the Ministry and its partners—the foreign companies—to identify potential recruits from the contracted company for the purpose of making them agents of Russian high tech and industrial espionage.

Finally, it will be naive to hope that President Yeltsin will decide to cut Russian intelligence substantially. In addition, practically all the new countries, the former republics of the U.S.S.R., can be expected to conduct external intelligence on their own with U.S. technology as a prime target. Allegedly the Ukraine already has hundreds of intelligence officers and is training the younger generation.

The intelligence services of the former republics will almost assuredly coordinate their work. An important part of it will be industrial espionage.

This concludes my prepared statement, and I will be very glad to answer any questions.

Mr. GLICKMAN. OK. Thank you all for your testimony.

[The prepared statement of Mr. Levchenko follows:]

PREPARED STATEMENT OF STANISLAV LEVCHENKO

Mr. Chairman and Members of the Subcommittee:

I am here today to discuss the threat of foreign intelligence agencies conducting economic espionage against U.S. industry. With Russia and the surrounding states' economies crumbling, there is little money for advanced business technologies and designs. Intelligence groups will have to steal them or obtain them with bribes, in order to gain competitiveness. My testimony is based on knowledge gained through many years of working for the Communist Party of the Soviet Union and for the KGB, as well as my ongoing research on these topics.

My Experience with Soviet Intelligence

Starting in the 1960's, I began working as a specialist on Asia for two Soviet Communist Party and intelligence fronts--the Soviet Peace Committee and the Soviet Afro-Asian Solidarity Committee. Both were totally controlled by the International Department in the Central Committee of the Communist Party of the Soviet Union and the KGB.

In the mid-1960s, I was ordered to become a reserve intelligence officer with the GRU--the Soviet military intelligence service. In the early 1970s, I was recruited as a KGB External Intelligence officer. Later, probably because of my educational background in Japanese language, I went to Japan as a field officer, under cover as the Tokyo bureau chief of a Soviet magazine--New Times. Part of my field officer responsibilities included recruiting agents in the Japanese government, political parties, and the mass media;

planting and spreading false information that was beneficial to USSR foreign policy goals; and also planting forgeries of foreign government documents, in an effort to compromise their policy towards Japan.

In Tokyo, I was in touch with KGB external intelligence officers who dealt with counterintelligence, political, and high technology issues. Naturally, I became friends with several of the 25 officers in high-tech intelligence stationed there. These 25 represented about 50 percent of the KGB residency in Tokyo, which indicates the importance that high-tech intelligence had for the USSR. One reason why the Soviets were very active in Japan is that they could acquire intelligence on U.S. technology plans through Japanese companies that were engaged in joint research with them. The other reason is that some of the Japanese companies had extensive knowledge of U.S. companies.

Since my defection, for political reasons, in 1979, to the United States, I have closely watched the new developments in Soviet-Russian intelligence. I have published three books, as well as many articles, analyzing new developments in the KGB.

Soviet-Russian Technology Intelligence:

Organizations and Activities

As you know, after the attempted coup last August, the KGB underwent and continues to undergo a major transformation. Its secret police organization was greatly reduced. Other KGB

organizations were reduced and became independent organizations. In place of the KGB, the Ministry of Security was established. Part of its role continues to be foreign counterintelligence, an effort that allegedly has not been reduced. Among other parts is what was left of the secret police.

The Soviet-Russian foreign intelligence has changed its priorities. Several times last year, some Soviet officials indicated that their intelligence had changed its focus from collecting political and military information to economic or industrial information, in interviews to the Russian media. For decades, political intelligence was the number one priority. Now high-tech, industrial, and economic intelligence is the most important priority of the headquarters and of the residencies abroad. The economic situation of Russia and the surrounding states is severe. They do not have the resources nor the time for extensive research and development efforts necessary to compete in international markets. To survive, they will steal the proprietary secrets of foreign companies. Within the last few weeks, France, Belgium and the Netherlands have broken up industrial espionage rings operating on Moscow's behalf. In my view, these cases reveal increased Russian industrial espionage.

Only one part of the former KGB did not experience cuts or restructuring--the elite former First Chief Directorate. It is now an independent organization called the External Intelligence Service of Russia (EISR). Its director is Yevgeny Primakov,

Gorbachev's man, who is very active in the Parliament, protecting the interests of foreign intelligence, according to Russian Parliament members. He has broad support among moderates and hardliners.

I would like to give you a typical example of an EISR operation which would be used in Russia today. A Russian entrepreneur, trying to start a joint venture with a U.S. company, gets stalled by Russian bureaucracy. A Russian intelligence operative offers to help the entrepreneur in exchange for an agreement to hire an operative inside the company who will help establish contacts with foreign firms. However, the operative will also supply the External Intelligence Service of Russia with information on foreign competitors, their products, and research and development efforts. In cases involving U.S. firms, the agents recruited by Russians can be U.S. citizens. This enables them to operate more naturally with the U.S. companies, facilitating the collection of secrets. Such operations will be subtle, frequently under the guise of offering to help U.S. businesses get established in Russia and other areas. Further, many Russian businessmen will make such agreements in exchange for help and Russian intelligence can get hundreds of new covers for its operatives. In some cases, Russian intelligence will establish joint ventures and separate firms exclusively employing its officers for the purpose of collecting corporate intelligence.

Further, the United States will have increasing difficulty detecting Russian intelligence officers among the masses leaving the impoverished Russia. Thousands of Russian engineers, scientists, and specialists in almost every field of technology and industry, as well as fired KGB officers, are travelling abroad in search of employment.

One part of the External Intelligence Service of Russia--Service "T"--concentrates on high-tech intelligence. It consists of three branches. One, its operational branch, dispatches intelligence officers to the residencies abroad and to work under cover on the territory of Russia. It also controls their operations. Two, its analytical branch, coordinates the collection effort on a global basis and issues a "shopping list" containing names of the foreign high-tech companies and their products. This list is as thick as the "Yellow Pages." Three, its research institute, which reportedly employs up to one thousand specialists with and without military rank, sorts out acquired technology and forwards it to appropriate ministries and research facilities of the Russian Academy of Sciences.

Before perestroika, the KGB had an elaborate list of major U.S. defense companies. In the late 1970s and early 1980s, General Electric was the number one target for acquisition of technology. The KGB also targeted Boeing, Lockheed, Rockwell International, Martin Marietta, and others.

For many years until recently, the supreme authority in issuing the guidelines for overt and covert acquisition of Western technology was the Soviet Politburo. Technology acquisition, prioritization, and coordination were controlled by the most powerful organization in the former Soviet Defense Department--the Military Industrial Commission of the Presidium of the Council of Ministers. With the disbanding of the Communist party last year and structural changes in the huge Russian bureaucracy, it would be logical to assume that President Yeltsin's Council of Ministers began to coordinate the acquisition of Western technology.

Before major restructuring of the KGB last year, it assigned undercover officers to every Soviet ministry or organization involved in trading with the West. Most deputy chiefs of directorates and departments in the Ministry of Foreign Trade were, and most likely still are, intelligence officers. Russian intelligence scrutinizes most contracts signed by the ministry and its affiliates with the foreign companies to identify potential recruits from the contracted company for the purpose of making them agents in Russian high-tech and industrial espionage.

One of the most common methods that the Russian intelligence uses to acquire Western technology is through diversion of the technologies through various countries. According to one source, diversionary schemes accounted for 75 percent of all illegal high-technology shipments to the Soviet Union. When I was in Japan, the Soviet high-tech intelligence operatives in Japan sent more high-

tech items and technologies to Moscow than Russian specialists could digest.

Diversión schemes can be quite elaborate, as the following example shows. A Russian intelligence officer stationed in Tokyo might develop a relationship with a local Japanese businessman selling U.S. computer products. He learns that the Japanese businessman (1) has a small trading company in financial trouble, (2) can purchase U.S. computer parts, and (3) would be glad to resell the parts to free world countries. Thus, Service "T"--high tech intelligence--sends an agent, an Australian businessman, to Tokyo. The agent offers to pay cash for the U.S. computer parts, and he buys and ships the parts to Australia. In Australia, the agent ships the parts to a small trading company in another country, which is a front for the Russian intelligence operation. From there, the parts are sent to Russia.

Finally, it would be naïve to hope that President Yeltsin will decide to cut Russian intelligence substantially. In addition, practically all the new countries--the former republics of the USSR--can be expected to conduct external intelligence on their own, with U.S. technology as a prime target. Allegedly, the Ukraine already has hundreds of intelligence officers and is training the younger generation. The intelligence services of the former republics will almost assuredly coordinate their work. An important part of it will be industrial espionage.

This concludes my prepared statement, although I would be happy to answer any questions you may have.

Mr. GLICKMAN. I am going to ask questions of Mr. Levchenko first. You indicate in your statement, with the disbanding of the Communist Party last year and structural changes in the huge Russian bureaucracy, it would be logical to assume that President Yeltsin's Council of Ministers began to coordinate the acquisition of Western technology, and you seem to imply that in fact the economic intelligence, economic espionage, and intelligence activities may be on the increase by Russia and the other republics.

Does that imply that at the highest levels of the Russian Government a decision has been made to, basically, leapfrog technology by continuing theft and espionage that had been going on before the coup?

Mr. LEVCHENKO. Yes, I think so. I do not have documents to prove that, but without the Central Committee of the Communist Party of the Soviet Union which did run everything in the Soviet Union including tasking intelligence work, the only organization now which is left to give certain tasking and orders to intelligence is the Council of Ministers, and I would not be surprised that they are doing precisely that.

And Mr. Primakov, who is the Director of the Russian intelligence is very actively lobbying now among the rightwingers and moderates in the Russian Parliament also. He is a kind of an unusually energetic person in comparison to those people who are heading the remnants of other parts of the KGB.

Mr. GLICKMAN. And the purpose of this increased espionage is basically to allow Russia and the other republics to leapfrog technology. It is easier to steal it than do it on your own. Is that—

Mr. LEVCHENKO. That always was a policy of the Soviet Union, starting from the 1920's when it just started high tech intelligence against the United States. Then they managed to obtain illegally the technology of the atomic bomb and whatever. Unfortunately, they had many successes in working against this country.

What I would like to say is that at this very moment probably—we are not talking about tens of thousands of Russian spies, you know, 24 hours a day working in that field. What I meant in my statement and the statement which is attached to that is that it will be an increase in the high tech espionage, if not today, then tomorrow and day after tomorrow. And democracy still is not quite genuine in Russia, but the Russian media is extremely democratic. There is no question about it. And there are many very interesting indications in the Russian media related to that question.

Mr. GLICKMAN. But it would then surprise you if the number of agents both in this country and outside this country directed at getting economic intelligence, economic espionage would be going down, it would surprise you if that were the case then; right?

Mr. LEVCHENKO. I will be very much surprised. Mr. Chairman, there is one more interesting point here. Large parts of the KGB are gone and quite a few thousand of the KGB officers, primarily from the secret police, were fired, many without pension. So many of them are going now to entrepreneurship and they get into joint ventures. And now for the Soviet intelligence to plant their officers as entrepreneurs in all kinds of joint ventures is very easy, and I am afraid that law enforcement in this country will have quite a bit of headache because there is a very intensive traffic between

Russian and American businessmen. And to figure out who is who will be very difficult.

Mr. GLICKMAN. I will come back to you, Mr. Levchenko in 1 minute. I want to ask Mr. Phelps and Mr. Riesbeck what is the impact on U.S. industry of intelligence agency efforts to restrict the use and export of advanced encryption and fiber optic technology? However you want to handle that.

Mr. RIESBECK. Let me take that in two pieces. First, the encryption devices. The advent of modern digital-based telecommunications services has enabled us to become much more effective as a global competitor as we deploy this technology in businesses around the world. We hesitate to do so when that is done in a way that is very unsecure. Unsecured communications can be an impediment to our global competitiveness of reasonably significant proportion. The ability to quickly employ or deploy encryption devices is very important to us so that we are able to conduct business on a global leadership basis much more easily.

For example, we currently have two requests pending for approval for encryption devices for some of our international teleconferencing. The requests have been in to the Government since February. It is a very confusing process to us as to who has to approve the request. When it is approved, we have to get the approvals of the foreign government for the encryption device on that end. So what we are seeking is more of a partnership attitude with the agencies to help us deploy this quickly and protect our information as it flows back and forth.

The fiber optic technology question is a separate issue. Our position on that is that it is in the United States's best interest to deploy the modern enhanced service telecommunications systems throughout the globe. The United States leads the world not only in fiber, but also through our telecommunication companies in all forms of telecommunications services. In our opinion, we should rapidly deploy this throughout the world. As we do, we must give consideration to national security. We don't argue with that whatsoever. But we think the research to address national security concerns should be done rapidly so that it does not slow down the deployment of the technologies.

Mr. GLICKMAN. Mr. Phelps.

Mr. PHELPS. Let me just add a bit on the encryption side, if I could. On the Data Encryption Standard, or DES, IBM invented that. We license it at no cost. It is available around the world. Having created it and made it available, we find ourselves in sort of the ironic position of jumping through all kinds of hoops to market it. And our customers want it around the world. It is available around the world as a result. And we find that it is at least a marketing problem for us.

Beyond that, it requires us to have two lines of equipment, one with it and one without it, and that in this day and age is costly. And, when you add onto that the time it takes to get the individually validated licenses, you have got a problem on your hands from a business perspective.

There is a need for balance, as a lot of people have said. We agree with that. And we think there are legitimate needs on both sides of the classic public policy question.

Mr. GLICKMAN. So you at least acknowledge there is a classic public policy question. I couldn't get the Director of the FBI to say that.

Mr. PHELPS. Well, I think it is a dilemma that the country has to wrestle with, and I think the congressionally mandated study of that is an appropriate way to do it.

Mr. GLICKMAN. I just have one more question and I will yield to Mr. Fish.

Mr. Phelps, you indicate in your testimony that there will soon be a lobbying campaign to convince Congress to change U.S. laws protecting computer programs. Would you describe in detail what companies or countries are behind this lobbying campaign and how it will hurt U.S. companies?

Mr. PHELPS. I would like to do it a little bit by example, if I could. Here is a diskette of a computer program, a 3.5-inch diskette. It represents millions of dollars of creation in that little diskette. It costs about 80 cents to make that diskette. There are programs available as of yesterday from somewhere around \$89 to \$129 on the market that can take the code on this diskette and break it down into zeros and ones and turn it into code which humans can easily read and interpret and change.

A clever pirate can make superficial changes, much like plagiarizing a book. Take "Moby Dick" and turn it into a—change the fish or change the town and some of those things and market that, and that is a plagiarized version of that.

The people we talked about that are attempting to weaken this, it is—I guess I would say it is a worldwide effort because of the United States commanding lead in this area. There is unquestionable Japanese involvement in that they have been active in this area in Japan, have been for years, and in Europe. They formed, essentially, an association of non-European companies in Europe to argue this point during the recently developed European debates on software, called ECIS. Well, the American version of that is called ACIS. It is called the American Committee for Interoperable Systems, and what they have done is, having failed to get what they wanted in Europe, I would say, they are beginning a concerted campaign to get the U.S. Congress to weaken the intellectual property laws in this country to make it easier to break that code down under the guise, we think the unnecessary guise and the somewhat disingenuous guise of interoperability.

[Subsequently, Mr. Phelps requested that his response be revised as follows:]

Q. You indicate in your testimony that there will soon be a lobbying campaign to convince Congress to change U.S. laws protecting computer programs. Would you describe in detail what companies or countries would be behind this lobbying campaign and how would it hurt U.S. companies if it were successful.

A. Mr. Chairman, this diskette contains a program that cost tens of millions of dollars to create.

There are programs on the market -- available for \$129.95 -- that can take the recorded computer code on the diskette -- a series of 1s and 0s -- and turn it into code which humans can more easily read and understand. Once this is done, a clever pirate could make superficial, cosmetic changes to the code, and create a competing product that would substitute for the original and bypass the R&D required to create the original program.

This, Mr. Chairman, is like a pirate changing the names, locations, and dates in Moby Dick, using synonyms for the words, and claiming that the plagiarized work is original. However, like all plagiarism, it is theft of the copyrighted expression, plain and simple.

The agents I mentioned that are attempting to weaken computer program laws here and abroad would have you believe that weakening the laws protecting computer programs is required for innovation. Certain Japanese interests, and the Japanese government, have been arguing for such weakened protection first in their own country, as well as in forums like the GATT intellectual property negotiations. Moreover, they were very active behind the scenes in the debate over the European Community software directive.

There, a group of largely foreign companies formed an organization called the European Committee for Interoperable Systems, or ECIS. ECIS argued that laws protecting computer programs should permit computer programs to be stripped to their essence so that competitors could see precisely how they worked, allegedly to "independently" develop other products that would interoperate with them.

This stripping process -- known as decompilation -- is not required to create interoperable systems, as they would have you believe. But it is required to bypass research and development, for it is the easiest and cheapest way a pirate can manipulate the program and create a plagiarized copy. Its like stealing a novel that has a potential market of a quarter trillion dollars.

Recently, the offspring of the European ECIS was created here in the U.S. It is called the American Committee for Interoperable Systems, or ACIS. Having failed to obtain a decompilation exception that would permit them to go as far as they would have liked in Europe, ACIS is beginning a concerted campaign in the U.S. Congress to try and set a malicious precedent here. A

couple of U.S. companies have joined their efforts. We believe their policy objectives are misguided, and the vast majority of U.S. software companies that innovate -- rather than follow the work of others -- will be joining an effort to oppose these attempts by ACIS to legalize the theft of their software assets.

In the end, if they succeed, our foreign competitors will be the winners as America's greatest computer industry asset and opportunity is handed over. Please be skeptical of the arguments put forth. The health and diversity of the U.S. software industry is proof that the system is working.

Mr. GLICKMAN. Mr. Fish.

Mr. FISH. There was a time in the last 4 hours, 3 hours here that I thought I understood what was going on, and that was basically raised by our auditors with respect to cryptographic and other information technologies and the fact that the intelligence community was insisting on the development of a different standard for industry that was weaker. That was then explored with the intelligence community when they came to the table and I understood that Judge Sessions particularly was talking about digital telephony and how there is a danger that companies like IBM would be able to commit crimes without the FBI and intelligence agencies having access to the communications.

I understood up to then, if I am right. And I will ask you, Mr. Phelps, before we go any farther. So far am I right?

Mr. PHELPS. There has been a—this is a highly confusing area to everybody, I can tell you, having spent some time trying to get ready for this. We are talking about a variety of things. The Director of the FBI was specifically talking about the telephony, the digital telephony situation.

Mr. FISH. He was. OK. I will stop you there. So far, so good.

Now, you come along, and very good testimony, very tough testimony, very revealing. But we are talking here about Digital Signature Standards, which is encryption technology. And then once again there the U.S. Government is getting involved in using a different and unproven methodology. So that is a problem. Then you go ahead on page 8 and you say, "We've been asked to address issues surrounding the use and export of encryption technology." We get into something else here about Data Encryption Standards. So I understood up to that first point.

Now, would you go in and explain to me about these other phrases that you mention in your testimony—and maybe if someone reads the transcript of these hearings they too will have the benefit of understanding where the Government comes in and where the issue between companies like yourself and the intelligence community is that what enables them to have access to do what they consider their job is a severe handicap to American industry.

Mr. PHELPS. I am going to try, and, with your permission, assuming I don't do this very well, would like to come back to you and submit something to straighten this all out.

The digital telephony issue is one that we are involved in, and you heard our name mentioned, I think, by someone earlier. We are concerned with what we see as the inability to stop the march of technology, quite frankly. If you look at it historically, it really doesn't work very well. And we were concerned that the FBI has proposed, will propose, a legislative solution which may overreach, quite frankly. So we are participating with a broad coalition, and I think, Mr. Glickman, you may have read those names, I am not sure, of companies concerned with that particular issue. Now, let me move that to the side.

The data encryption issue is a technology, algorithms, mathematics, I suppose, that the company invented that allows data, data streams to not be deciphered, if you will, easily.

Mr. GLICKMAN. Scrambled.

Mr. PHELPS. It is a scrambling technique, and a lot of our customers around the world want that for all of the reasons you heard today. It is very hard in some cases to get export licenses for that equipment, albeit we invented it and albeit it is available around the world. And so we are somewhat at times, because of the procedures you go through, in a competitive disadvantage trying to get those licenses through the pipeline. That is the point I was on on that one.

The Digital Signature Standard, or DSS, that is a way of identifying that somebody who does something over here electronically is the same person that you think they are, as I understand it, and that is as far as I can go. It is just a case of there is a way to do it that we think is better than the new way the Government would like to do it, and that is a fairly simple point that we were asked to address.

And, if you need more than that, Mr. Fish, I am going to have to get people who really understand this to get back to you.

Mr. FISH. Well, I will stop there and read the transcript of your response a few times over before I put you to any further trouble. Thank you very much. You have been helpful.

Mr. GLICKMAN. Mr. Phelps, you said in your statement when you talked about these activities have resulted in losses to IBM in the billions, and I think that is the first time anybody has ever publicly talked about how expensive this proposition is of theft of corporate proprietary assets, from—you say from many quarters, however, from competitors, from governments seeking to bolster national industrial champions, even employees.

Can you allocate the percentage of the loss of that billions would be to folks outside the United States, governments or foreign companies?

Mr. PHELPS. Not very easily. I don't have that available to me.

Let me just say this. It is a problem that exists on all those levels concurrently. I can't tell you how much of it—and it is also hard to say where it started and where it stopped, and once something is lost it gets repetitively lost. In the case of software, for example, once the horse is out of the barn, of course, it is replicated and you get losses on top of losses, and it is virtually impossible to see where that would end as it circles the globe.

In many cases, some of the foreign activities, which I really cannot get into for a lot of reasons which I spelled out, are caused by employees, as you heard somebody say today, in the United States who left the business with confidential information with them and sold it. So what is that? Is that a U.S. problem or a foreign problem ultimately? It is both is I guess the right answer. So I can't do that allocation for you.

Mr. GLICKMAN. Well, I would say that these hearings, I have sat in about half of them, and they have been very useful. Above all there ought to be a wake-up call to American business to be far more alert, and to how they just do their normal operations. Because there are people out there, a lot of them, outside this country operated or owned by foreign governments who are there to take what they have got.

So simple things like locking the door and watching how loud you talk and where you leave material, those kinds of things are

going to have to be done now. I mean, this is a very competitive world and we can no longer assume that everybody we see is just pleasant, nice and not going to fight this game like it is a war.

Second, we go to the next step as to what level of protective standards should be offered and should the Government be helping in that. And it does appear to me, based upon the testimony that I have heard together with the fact that Mr. Brooks and I basically coauthored the Computer Security Act of 1987, is that Government, and I speak generically, is not cooperating with the private sector very well to protect proprietary and sensitive information that is used to produce lots of jobs in this country. In fact, in many cases the Government may be hurting the development of those technologies.

At the same time, number three, we know that there has to be some public policy role for law enforcement. I recognize that as well.

And fourth, as Mr. Levchenko talks about, is that the mere fact that the cold war has "ended" in its classical way does not mean that similar threats don't continue to face the United States from even similar sources. Maybe the motivations are different.

So I think this has been very helpful testimony, and I know that we intend to work on some legislative initiatives that may deal with at least some of the problems.

I have got a closing statement. I want to thank all of the witnesses for their excellent testimony. Judging from what we have heard, I believe there is a consensus building in industry and Government that foreign economic espionage is a growing threat to U.S. industry.

In this age of global competition, we as a nation must face these problems squarely and with determination if we are going to maintain our standing in the world marketplace. I am heartened to know that the FBI, CIA, and NSA are focusing their attention on this important problem. Clearly, the U.S. Government has a major role in combating this problem, and I would like to explore further ways in which we can improve the apprehension and prosecution of those who conduct foreign economic espionage activities against American companies.

One of the troubling questions remaining from today's hearing is the question of data encryption. We need to examine closely the claims by industry that the current attempts by U.S. intelligence and law enforcement agencies to restrict this technology will seriously impair privacy and technological development in our country. I hope to explore this matter further with representatives of U.S. industry and other experts at our upcoming hearing on May 7.

That last statement was Chairman Brooks' closing statement.

The hearing is adjourned.

[Whereupon, at 1:20 p.m., the subcommittee adjourned, to reconvene subject to the call of the Chair.]